#2

1990.62597 PATENT

JC511 U.S. PTO
09/159833
09/24/98

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)
)
Applicant: Utsumi et al.)
)
Serial No.)
)
Filed: September 24, 1998)
)
For: STORING APPARATUS AND PASSWORD CONTROL METHOD)
)
Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Asst. Comm. for Patents, Washington, D.C. 20231, on this date.

09/24/98
Date

Express Mail Label No.: EM044996791US

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

CLAIM FOR PRIORITY

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 10-065281

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By James K. Folker

James K. Folker
Reg. No. 37,538

September 24, 1998
Sears Tower - Suite 8660
233 South Wacker Drive
Chicago, IL 60606
(312) 993-0080

PATENT OFFICE
JAPANESE GAVERNMENT

This is certify that the annexed is a true copy of the following application as filed with the Office.

Date of Application : March 16, 1998

Application Number : Patent Application No.Heisei 10-065,281

Applicant (s) : Fujitsu Limited

July 24, 1998

Commissoner, Takeshi Isayama

Patent Office

Certificate No.Hei 10-3056440

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年 ３月１６日

出 願 番 号
Application Number: 平成１０年特許願第０６５２８１号

出 願 人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９８年 ７月２４日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１０－３０５６４４０

【書類名】　特許願

【整理番号】　9800549

【提出日】　平成10年 3月16日

【あて先】　特許庁長官殿

【国際特許分類】　G11B 19/04

【発明の名称】　記憶装置及びそのパスワード制御方法

【請求項の数】　21

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　内海　研一

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　内田　好昭

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小林　弘幸

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100079359

【弁理士】

【氏名又は名称】　竹内　進

【電話番号】　03(3432)1007

【選任した代理人】

【識別番号】　100093584

【弁理士】

【氏名又は名称】　宮内　佐一郎

【電話番号】　03(3432)1007

【手数料の表示】

【予納台帳番号】　009287

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704823

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　記憶装置及びそのパスワード制御方法

【特許請求の範囲】

【請求項１】

媒体に記録された情報のアクセスをパスワードにより保護するための記憶装置に於いて、

デフォルト入力パスワード及びクアセス保護用パスワードを保存するパスワード保存部と、

ユーザからのパスワード入力がない場合は、前記デフォルト入力パスワードをユーザ入力パスワードに置き換えて前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、ユーザ入力パスワードと前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御するパスワード検証部と、

を備えたことを特徴とする記憶装置。

【請求項２】

請求項１記載の記憶装置に於いて、前記パスワード保存部で前記デフォルト入力パスワードとアクセス保護用パスワードに同じ値を保存していた場合、前記パスワード検証部は、ユーザのパスワード入力がなくとも、前記デフォルト入力パスワードをユーザ入力パスワードに置き代えたアクセス保護用パスワードとの照合によりアクセスを許可することを特徴とする記憶装置。

【請求項３】

請求項１記載の記憶装置に於いて、前記パスワード保存部は、更にユーザ入力のパスワードを格納するユーザ入力パスワード領域を有し、

前記パスワード検証部は、

電源投入、コマンドリセット、エラーリセット、更に媒体挿入等の装置の使用

【請求項６】

請求項１記載の記憶装置に於いて、

前記パスワード保存部は、前記デフォルト入力パスワードとアクセス保護用パスワードを前記媒体に保存し、

前記パスワード検証部は、装置の使用開始時に前記媒体から前記デフォルト入力パスワードとアクセス保護用パスワードを装置本体に読み出してアクセス保護を制御することを特徴とする記憶装置。

【請求項７】

請求項１記載の記憶装置に於いて、

前記パスワード保存部は、前記デフォルト入力パスワードを装置本体の不揮発性メモリに保存すると共に、前記アクセス保護用パスワードを媒体に保存し、

前記パスワード検証部は、装置の使用開始時に前記媒体から前記アクセス保護用パスワードを装置本体に読み出してアクセス保護を制御することを特徴とする記憶装置。

【請求項８】

請求項１記載の記憶装置に於いて、

前記パスワード検証部は、前記アクセス保護用パスワードを装置本体の不揮発性メモリに保存すると共に、前記デフォルト入力パスワードを媒体に保存し、

前記パスワード処理部は、装置の使用開始時に前記媒体から前記デフォルト入力パスワードを装置本体に読み出してアクセス保護を制御することを特徴とする記憶装置。

【請求項９】

請求項５乃至７のいずれかに記載の記憶装置に於いて、前記媒体は通常のリードコマンド及びライトコマンドでアクセスすることのできない特定領域に前記パスワードを保存するパスワード保存領域を設けたことを特徴とする記憶装置。

【請求項１０】

請求項１記載の記憶装置に於いて、更に、上位装置からの専用コマンドに基づいて前記デフォルト入力パスワード又は前記アクセス保護用パスワードを書き替えるパスワード書替部を備えたことを特徴とする記憶装置。

【請求項１１】

請求項５乃至７のいずれかに記載の記憶装置に於いて、前記媒体は装置本体の内部に固定的に収納された媒体であることを特徴とする記憶装置。

【請求項１２】

請求項５乃至７のいずれかに記載の記憶装置に於いて、前記媒体は装置本体に対し着脱自在なリムーバブル媒体であることを特徴とする記憶装置。

【請求項１３】

請求項１記載の記憶装置に於いて、

前記パスワード保存部は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワードを保存し、

前記パスワード検証部は、照合一致が得られたアクセス保護用パスワードの種別に対応した通常コマンドによるアクセスを許可することを特徴とする記憶装置。

【請求項１４】

請求項１３記載の記憶装置に於いて、

前記パスワード保存部は、アクセス保護用パスワードとして、読出及び書込コマンドによるアクセスを許可する書込読出パスワードと、読出コマンドによるアクセスのみを許可する読出オンリーパスワードとを保存し、

前記パスワード検証部は、前記書込読出パスワードの照合一致が得られた場合は通常の書込コマンド又は読出コマンドによるアクセスを許可し、前記読出オンリーパスワードの照合一致が得られた場合は通常の読出コマンドのみによるアク

セスを許可することを特徴とする記憶装置。

【請求項１５】

請求項１記載の記憶装置に於いて、更に、デフォルト入力パスワードに有効期間を設定する有効期間設定部を設けたことを特徴とする記憶装置。

【請求項１６】

請求項１５記載の記憶装置に於いて、前記有効期間設定部は、装置の使用回数をカウンタで計数し、前記カウンタの値が所定値に達したとき、前記デフォルト入力パスワードをそれまでのデフォルトパスワードとは異なる値に強制的に変更することを特徴とする記憶装置。

【請求項１７】

請求項１５記載の記憶装置に於いて、前記有効期間設定部は、有効期限の時刻を設定し、装置を使用した際の現在時刻が前記有効期限を超えていたとき、前記デフォルト入力パスワードをそれまでのデフォルトパスワードとは異なる値に強制的に変更することを特徴とする記憶装置。

【請求項１８】

媒体に記録された情報のアクセスをパスワードにより保護するためのパスワード制御方法に於いて、

デフォルト入力パスワード及びアクセス保護用パスワードを保存するパスワード保存過程と、

ユーザからのパスワード入力がない場合は、前記デフォルト入力パスワードをユーザ入力パスワードに置き換えて前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、前記ユーザ入力パスワードと前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御するパスワード検証過程と、

を備えたことを特徴とするパスワード制御方法。

【請求項１９】

請求項１８記載のパスワード制御方法に於いて、前記デフォルト入力パスワードとアクセス保護用パスワードに同じ値を保存していた場合、前記パスワード検証過程は、ユーザのパスワード入力に先立って、前記デフォルト入力パスワードの値をユーザ入力パスワードに複写して、これとアクセス保護用パスワードを照合することによりアクセスを許可又は不許可することを特徴とするパスワード制御方法。

【請求項２０】

請求項１８記載のパスワード制御方法に於いて、

前記パスワード保存過程は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワードを保存し、

前記パスワード検証過程は、照合一致が得られたアクセス保護用パスワードの種別に対応した通常コマンドによるアクセスを許可することを特徴とするパスワード制御方法。

【請求項２１】

請求項１８記載のパスワード制御方法に於いて、更に、デフォルト入力パスワードに有効期間を設定する有効期間設定処理を設けたことを特徴とするのパスワード制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータやワードプロセッサ、電子ブック等の情報処理機器に接続するハードディスクドライブや光ディスクドライブ等の記憶装置及びパスワード制御方法に関し、特に、媒体に記録された情報のアクセスをパスワードにより保護するための記憶装置及びパスワード制御方法に関する。

【０００２】

【従来の技術】

従来、ハードディスクドライブや光ディスクドライブ等の記憶装置にあっては、パスワードを使用して媒体に記録したデータを保護するようにしている。即ち、記憶装置の媒体に対するデータの読み書きを特定の人にだけ認め、他の人にはアクセスさせないためにパスワードによって本人確認を行っている。

【０００３】

例えば、記憶装置あるいは記憶媒体に予めパスワードを書き込んで保存しておき、記憶装置を使用する時にユーザがパスワードを入力し、ユーザ入力のパスワードと装置側に保存したパスワードとが一致すると、記憶媒体への書込コマンド又は読出コマンドを受け付ける。パスワードが不一致であれば書込コマンド又は読出コマンドを受け付けず、エラーを返すものである。

【０００４】

このようなパスワードにより個人を認証するシステムは、記憶装置のアクセス保護に限らず、データ通信システムでの端末装置の使用など多くの場合に用いられる。またパスワードを用いた保護システムは、簡単に実装できる技術でありながら、一定の効果を期待できるので広く使われている。

【０００５】

【発明が解決しようとする課題】

しかしながら、このようなパスワードを用いたアクセス保護は、広く使われる故に、個々人のユーザは多数のパスワードを持つことになり、全てのパスワードを覚えておくのが困難な場合も多い。このため、ユーザが自分で使用しているパスワードを忘却した場合、正しいユーザであってもアクセスできなくなってしまうという問題がある。

【０００６】

そこでユーザはスワードを手帳などに記録しておき、装置を使う度に手帳のパスワードを確認するといった使い方も見受けられる。これでは、ユーザの手帳を

盗み見ることによってパスワードが知れてしまうという問題がある。

また、パスワードを用いたアクセス保護は、アクセスの度にパスワード入力を促すことを想定しているため、職場の同僚などの第三者がパスワードに接する機会も多い。

【０００７】

このような問題は、装置を使用する際に常にパスワードの入力を必要とする操作に伴う問題であり、パスワードでアクセス保護を行いながら、更に、使用者がパスワードを入力する頻度を少なくできるような技術が求められる。

この問題を解決するものとして、任意の使用時点でパスワードを削除してパスワートによるアクセス保護を止め、アクセス保護が必要になれば改めてパスワードを設定する手法が考えられる。即ち、保護が必要な期間だけパスワードを設定してアクセス保護を受ける方法である。

【０００８】

しかし、この方法には、次の問題がある。第１に、パスワードを再設定するときに、先のパスワードとは異なるパスワードにしてしまうことが多いので、パスワード管理が繁雑になる。つまり、最新のパスワードが何であったか忘れてしまいやすい。第２に、パスワードを再設定する場面が第三者に盗み見られる危険がある。

【０００９】

本発明は、このような問題点に鑑みてなされたもので、パスワードによるアクセス保護の機能を損うことなく、使用場面によってはユーザのパスワード入力を必要とすることなくアクセス許容されるようにした記憶装置及びパスワード制御方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】

図１は本発明の原理説明図である。

図１（Ａ）は、媒体に記録された情報のアクセスをパスワードにより保護するための本発明が対象とする記憶装置４４であり、パスワード保存部４５とパスワ

ード検証部４８を備える。パスワード保存部４５は、デフォルト入力パスワード６０及びアクセス保護用パスワードを保存する。

【００１１】

パスワード検証部４８は、ユーザからのパスワード入力がない場合は、デフォルト入力パスワード６０をユーザ入力パスワード６６に置き換えてアクセス保護用パスワード６２との比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、ユーザ入力パスワード６６とアクセス保護用パスワード６２との比較照合によりアクセス保護を制御する。

【００１２】

特に、パスワード保存部４５でデフォルト入力パスワード６０とアクセス保護用パスワード６２に同じ値を保存していた場合、パスワード検証部４８は、ユーザのパスワード入力がなくとも、デフォルト入力パスワード６０をユーザ入力パスワード６６に置き換えてアクセス保護用パスワード６２との照合によりアクセスを許可する。

【００１３】

このように本発明は、記憶装置側にデフォルト入力パスワードを格納し、ユーザからのパスワード入力がない場合は、デフォルト入力パスワードをユーザ入力パスワードと見做してパスワード検証を行うため、デフォルト入力パスワードとアクセス保護用パスワードを同じ値にしておくことによって、ユーザがパスワード入力しなくともアクセス保護は許可されて通常コマンドによるアクセスができ、ユーザによるパスワード入力を省略できる。

【００１４】

パスワード保存部４５は、更にユーザ入力パスワード６６を格納するユーザ入力パスワード領域６５を有し、パスワード検証部４８は、電源投入、コマンドリセット、エラーリセット、更に媒体挿入等の装置の使用開始時に、デフォルト入力パスワード６０を読み出してユーザ入力パスワード領域６５に書き込み、次にユーザ入力パスワード領域６５のデフォルト入力パスワード６０とアクセス保護用パスワード６２とを照合一致に基づいてアクセス許可又は不許可を確立する。

【００１５】

アクセス許可確立後は、ユーザのパスワード入力がある毎に、ユーザ入力パスワード領域６５にユーザ入力パスワード６６を書き込み、次にアクセス保護用パスワード６２との照合一致に基づいてアクセス許可又は不許可を確立する。

またユーザがパスワードの入力操作を必ず必要とする形態とした場合、パスワード検証部４８は、装置の使用開始時に、デフォルト入力パスワード６０を読み出してユーザ入力パスワード領域６５に書き込んだ状態でユーザのパスワード入力を待ち、ユーザのパスワード入力があった場合は、ユーザ入力パスワード領域６５のデフォルト入力パスワード６０をユーザ入力パスワード６６で上書きした後にアクセス保護用パスワード６２との照合比較し、アクセス保護を制御する。

【００１６】

勿論、デフォルトパスワードとアクセス保護パスワードが異なる時は、ユーザが正しいアクセス保護パスワードを入力しない限り、アクセスは保護される。

パスワード保存部４５は、図１（Ａ）のように、デフォルト入力パスワード６０とアクセス保護用パスワード６２を媒体５２に保存する。このときパスワード検証部４８は、装置の使用開始時に媒体からデフォルト入力パスワード６０とアクセス保護用パスワード６２を装置内部のワークメモリに読み出してアクセス保護を制御する。

【００１７】

またパスワード保存部４５は、デフォルト入力パスワード６０とアクセス保護用パスワード６２を装置本体の不揮発性メモリ４０に保存してもよい。

更に、パスワード保存部４５は、デフォルト入力パスワード６０を装置本体の不揮発性メモリ４０に保存すると共に、アクセス保護用パスワード６２を媒体５２に保存してもよい。この場合、パスワード検証部４８は、装置の使用開始時に媒体５２からアクセス保護用パスワード６２を装置本体のワークメモリに読み出してアクセス保護を制御する。

【００１８】

更に、パスワード保存部４５は、アクセス保護用パスワード６２を装置本体の不揮発性メモリ４０に保存すると共に、デフォルト入力パスワード６０を媒体５２に保存し、この場合、パスワード検証部４８は、装置の使用開始時に媒体５２

からデフォルト入力パスワード６０を装置本体に読み出してアクセス保護を制御する。

【００１９】

媒体５２は通常のリードコマンド及びライトコマンドでユーザがアクセスすることのできない特別領域にパスワードを保存するパスワード保存領域６８を設ける。これによってパスワードが通常のリードコマンドで読み出されたり、ライトコマンドで書き替えられることを防止する。

更に、上位装置４２からの専用コマンドに基づいてデフォルト入力パスワード６０又はアクセス保護用パスワード６２を書き替えるパスワード書替部５４を設ける。媒体は装置本体の内部に固定的に収納された媒体であってもよいし、装置本体に対し着脱自在なリムーバブル媒体であってもよい。

【００２０】

パスワード保存部４５は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワード６２を保存し、パスワード検証部４８は、照合一致が得られたアクセス保護用パスワード６２の種別に対応した通常コマンドによるアクセスを許可する。

例えばパスワード保存部４５は、アクセス保護用パスワード６２として、読出及び書込コマンドによるアクセスを許可する書込読出パスワード６２と、読出コマンドによるアクセスのみを許可する読出オンリーパスワード６４とを保存し、パスワード検証部４８は、書込読出パスワード６２の照合一致が得られた場合は通常の書込コマンド又は読出コマンドによるアクセスを許可し、読出オンリーパスワード６４の照合一致が得られた場合は通常の読出コマンドのみによるアクセスを許可する。

【００２１】

更に、デフォルト入力パスワード６０に有効期間を設定する有効期間設定部を設ける。このようにパスワード入力を省略できる状態を一定期間だけに限定して継続させることにより、不用意な長期間に亘って無防備な状態が続くことを防止できる。

また逆に一定期間経過後に、パスワードが省略できる状態とする使い方もでき

る。即ち、一定期間後にデフォルトパスワードをアクセス保護パスワードと等しくなるようにすることで、一定期間後にパスワードを入力しなくともアクセスできる状態とすることができる。

【００２２】

有効期間設定部は、装置の使用回数をカウンタで計数し、カウンタの値が所定値に達したとき、デフォルト入力パスワード６０を異なる値に強制的に変更して使えなくする。また有効期間設定部は、有効期限の時刻を設定し、装置を使用した際の現在時刻が有効期限を超えていたとき、デフォルト入力パスワード６０を異なる値に強制的に変更して使えないようにする。

【００２３】

また本発明は、媒体に記録された情報のアクセスをパスワードにより保護するためのパスワード制御方法を提供するもので、次の手順から成る。

デフォルト入力パスワード６０、アクセス保護用パスワード６２及びユーザ入力パスワード６６を保存するパスワード保存過程；

ユーザからのパスワード入力がない場合は、デフォルト入力パスワード６０をユーザ入力パスワード６６に置き換えてアクセス保護用パスワード６２との比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、ユーザ入力パスワード６６とアクセス保護用パスワード６２との比較照合によりアクセス保護を制御するパスワード検証過程；

とを備える。

【００２４】

ここでデフォルト入力パスワード６０とアクセス保護用パスワード６２に同じ値を保存していた場合、パスワード検証過程は、ユーザのパスワード入力がなくとも、デフォルト入力パスワード６０をユーザ入力パスワードに置き換えてアクセス保護用パスワード６２との照合によりアクセスを許可する。

またパスワード保存過程は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワード６２を保存し、パスワード検証過程は、照合一致が得られたアクセス保護用パスワード６２の種別に対応した通常コマンドによるアクセスを許可することを特徴とする。更に、デフォルト入力パスワード６０に有効期間を設

定する有効期間設定過程を設ける。これ以外の詳細は装置構成と同じである。

【００２５】

【発明の実施の形態】

＜目次＞

１．固定媒体の記憶装置

２．リムーバブル媒体の記憶装置

１．固定媒体の記憶装置

図２は本発明のデフォルト入力パスワードを用いたパスワード保護が適用されるハードディスクドライブのブロック図であり、ハードディスクドライブにあっては、磁気ディスク媒体がドライブ本体に固定的に内蔵されている。

【００２６】

図２において、ハードディスクドライブ（ＨＤＤ）はエンクロージャ１０とコントロールボード１２で構成される。エンクロージャ１０にはヘッドＩＣ回路１４が設けられ、この実施形態にあっては４つのヘッドアッセンブリィ１６－１～１６－４を接続している。

ヘッドアッセンブリィ１６－１～１６－４にはインダクティブヘッドを用いた記録ヘッドとＭＲヘッド等を用いた再生ヘッドが設けられている。またエンクロージャ１０にはヘッドアクチュエータを駆動するＶＣＭ１８、及びディスク媒体を回転するスピンドルモータ２０が設けられる。

【００２７】

エンクロージャ１０のヘッドＩＣ回路１４に対しては、コントロールボード１１側にライトチャネル回路２８とリードチャネル回路２６が設けられている。ライトチャネル回路２８とリードチャネル回路２６に対してはハードディスクコントローラ２４が設けられ、ハードディスクコントローラ２４にはフォーマッタやＥＣＣ回路等が内蔵されている。

【００２８】

ハードディスクコントローラ２４はインタフェース回路３６に接続され、上位

装置としてのホスト側とのデータ伝送によってホストからのライトデータの供給及びホストに対するリードデータの転送を行っている。このインタフェース回路３６としては、ＳＣＳＩインタフェース、ＡＴＡインタフェース、ＡＴＡＰＩインタフェース、ＳＩＳＩ等、適宜のインタフェースを使用することができる。

【００２９】

この実施形態にあっては、ディスク媒体の記録方式としてゾーン分割による定密度記録方式（ＺＣＤＲ）を採用しており、ディスク媒体のシリンダを所定シリンダ数ごとにゾーン分割し、各ゾーンごとに異なった周波数を予め設定している。このため、周波数シンセサイザとして機能するＰＬＬ回路３０が設けられ、リード動作またはライト動作の際のシリンダアドレスから対応するゾーン周波数をセットすることで、ライトチャネル回路２６及びリードチャネル回路２８に対するクロック供給を行う。

【００３０】

ハードディスクドライブの全体的な制御はＭＣＵ（メインコントロールユニット）２２が行う。ＭＣＵ２２にはバスを介してハードディスクコントローラ２４及びインタフェース回路２８が接続され、更にワークメモリとして機能するＲＡＭ３８と不揮発性メモリとして機能するフラッシュＲＯＭ４０を接続している。

ＭＣＵ２２は、ホストからの各種コマンドを受領して解読し、ハードディスクドライブに対する通常コマンドによる通常リード／ライト指示、及びエンクロージャ１０に設けているＶＣＭ１８によるヘッド位置決め制御のためのサーボコントローラ３４に対する制御指示を行う。

【００３１】

ＶＣＭ１８の駆動によるヘッド位置決め制御を行うため、サーボ復調回路３２とサーボコントローラ３４が設けられている。この実施形態にあっては、ディスク媒体のサーボ情報としてデータ面サーボ方式を採用しており、このためリードチャネル回路２６に対する再生信号からサーボ情報を分離して、サーボ復調回路３２でヘッド位置情報を復元している。

【００３２】

図３は、図２のコントロールボード１２に設けたＭＣＵ２２のプログラム制御

によって実現されるパスワードを用いた本発明によるアクセス保護の機能ブロック図である。

図３において、上位装置４２に対する外部記憶装置としてハードディスクドライブ４４が接続されている。ハードディスクドライブ４４の不揮発性メモリ４０には、この実施形態にあってはパスワード保存領域４５が設けられ、このパスワード保存領域４５の中にデフォルト入力パスワード（ＤＰＷ）６０、書込読出パスワード（ＰＡ０）６２、及び読出オンリーパスワード（ＰＡ１）６４を保存している。またＲＡＭを用いたワークメモリ３８にはユーザ入力パスワード（ＵＰＷ）６６を格納するためのユーザ入力パスワード格納領域６５が設けられている。

【００３３】

ここで不揮発性メモリ４０に格納した書込読出パスワード６２及び読出オンリーパスワード６４は、上位装置４２からのユーザ入力によるユーザ入力パスワード６６との照合によりパスワード照合一致が得られた時に、各パスワードで定められたアクセスを許容するアクセス保護用のパスワードである。

即ち書込読出パスワード６２は、ユーザ入力パスワード６６との照合一致が得られた時に、ディスク媒体５２に対する通常のライトコマンドによる書込アクセスまたは通常のリードコマンドによるリードアクセスを許可する。これに対し読出オンリーパスワード６４は、ユーザ入力パスワード６６との照合一致が得られた時に、ディスク媒体５２に対する通常のリードコマンドによる読出アクセスのみを許容する。即ち書込読出パスワード６２及び読出オンリーパスワード６４は、アクセス保護と同時にアクセス種別を決めるパスワード機能を持っている。

【００３４】

このようなアクセス保護用の書込読出パスワード６２と読出オンリーパスワード６４を用いたアクセス保護は、従来のパスワードを用いたアクセス保護と同じであるが、これに加えて本発明にあっては、新たにデフォルト入力パスワード６０を保存している。

デフォルト入力パスワード６０は、上位装置４２からユーザ入力パスワード６６を受けなくともハードディスクドライブ４４におけるディスク媒体５２のアク

セスを許可するパスワードである。具体的には、ハードディスクドライブ４４の使用開始時に上位装置４２からユーザによるパスワード入力がなかった場合には、不揮発性メモリ４０に保存しているデフォルト入力パスワード６０をユーザ入力パスワード６６とみなして、アクセス保護用パスワードである書込読出パスワード６２及び読出オンリーパスワード６４との比較照合を行う。

【００３５】

この比較照合により、デフォルト入力パスワード６０が例えば書込読出パスワード６２に一致すれば、書込読出パスワード６２で指定されるアクセス種別として通常コマンドによる書込アクセス及び読出アクセスを許可する。このようなデフォルト入力パスワード６０を用いたアクセス保護を行うため、ハードディスクドライブ４４には、コマンド処理部４６、パスワード検証部４８及びアクセス実行部５０が設けられている。

【００３６】

コマンド処理部４６は、上位装置４２からのコマンドを受信して解読し、必要な処理を行う。例えば装置の使用開始時には、ユーザがパスワードを入力すると、ユーザが入力したパスワードがパスワード転送コマンドによりハードディスクドライブ４４に送られることから、このパスワード転送コマンドをコマンド処理部４６で解読し、コマンドパラメータとして取得したユーザ入力パスワード６６をワークメモリ３８のユーザ入力パスワード格納領域６５に書き込む。

【００３７】

またコマンド処理部４６にはパスワード書替部５４が設けられており、不揮発性メモリ４０に格納されているデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４の書替えを、上位装置４２に対するインタフェースでサポートされるパスワード書替専用のコマンドにより書替え変更ができる。このパスワード書替えコマンドとしては、例えばＳＣＳＩインタフェースであればフォーマットコマンドやベンダユニークコマンドが使用できる。

【００３８】

パスワード検証部４８には、パスワード照合部５６とアクセスモード設定部５８が設けられる。パスワード照合部５６は、ハードディスクドライブ４４の使用

開始時に、まず不揮発性メモリ４０からデフォルト入力パスワード６０を読み出してワークメモリ３８のユーザ入力パスワード格納領域６５に書き込む。このため装置使用開始時に、まずユーザ入力パスワード６６としてはデフォルト入力パスワード６０の値がセットされる。

【００３９】

ワークメモリ３８のユーザ入力パスワード格納領域６５にユーザ入力パスワード６６としてデフォルト入力パスワード６０を書き込んだ後の処理は、次の２つがある。

①ユーザのパスワード入力を待たずにパスワード照合を行う処理

②ユーザのパスワード入力の実行操作を待ってパスワード照合を行う処理

まずユーザのパスワード入力を待たない処理にあっては、ワークメモリ３８のユーザ入力パスワード格納領域６５に対するデフォルト入力パスワード６０の書込みが済むと、ワークメモリ３８からユーザ入力パスワード６６と不揮発性メモリ４０から書込読出パスワード６２を読み出し、両者を照合する。

【００４０】

このパスワード照合で照合一致が得られると、書込読出パスワード６２で決まるアクセスモードをアクセスモード設定部５８で設定し、アクセス実行部５０に対し上位装置４２からの通常のライトコマンドによる書込アクセス及びリードコマンドによる読出アクセスの許可状態を確立する。

一方、上位装置４２からのユーザによるパスワード入力操作を待つ処理にあっては、パスワード照合部５６でワークメモリ３８のユーザ入力パスワード格納領域６５にデフォルト入力パスワード６０を書き込んだ後、上位装置４２からのパスワード転送コマンドの受信を待つ。

【００４１】

コマンド処理部４６でパスワード転送コマンドが受信されると、コマンドパラメータとして受信したパスワードをワークメモリ３８のユーザ入力パスワード格納領域６５に上書きし、上書き後のユーザ入力パスワード６６と不揮発性メモリ４０の書込読出パスワード６２をパスワード照合部５６に読み出して照合し、照合一致が得られればアクセスモード設定部５８で書込読出モードをアクセスモー

ドとして設定する。

【００４２】

この場合、本発明にあっては、上位装置４２でユーザがパスワードの文字列を入力することなくパスワードの入力欄を空欄としたままパスワード入力を実行した場合については、実質的にユーザ入力パスワードの文字列が受信されなくとも、デフォルト入力パスワード６０に基づいたアクセス許可状態を確立する。

即ち、コマンド処理部４６で上位装置からパスワード転送コマンドを受信しても、コマンドパラメータとしてのパスワードの文字列が空き文字列であった場合、パスワード照合部５６は既にデフォルト入力パスワード６０に書き替えられているユーザ入力パスワード６６を読み出して不揮発性メモリ４０の書込読出パスワード６２と照合し、照合一致が得られれば、書込読出モードをアクセスモードとしてアクセスモード設定部５８により設定させる。

【００４３】

ここでハードディスクドライブ４４のパスワード検証部４８が不揮発性メモリ４０のデフォルト入力パスワード６０に基づいたアクセス保護を行う装置使用開始タイミングの内容としては、

①ハードディスクドライブ４４の電源投入時

②上位装置４２とのインタフェースによりコマンドリセットが行われた時

③ハードディスクドライブ４４が重大なエラー状態となり、内部リセットにより復帰した時

等がある。

【００４４】

図４は、図３のユーザのパスワード入力を必要としないアクセス保護の処理動作である。まず図３の不揮発性メモリ４０に保存されているデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４は、ハードディスクドライブ４４を低レベルフォーマットである初期化時に、予め定めた規定値、例えばオール０に初期化されている。

【００４５】

図４のハードディスクドライブ４４は、初期化状態にあるデフォルト入力パス

ワード６０及び書込読出パスワード６２であり、各パスワードは１６進で「００００００００ｈ」となっている。尚、図５には示していない図３の読出オンリーパスワード６４も同じ「００００００００ｈ」となっている。

このようなデフォルト入力パスワード６０及び書込読出パスワード６２が初期化により同じ値で保存された状態で、ハードディスクドライブ４４の電源が投入されたとすると、ハードディスクドライブ４４側において図３のパスワード検証部４８が、まずデフォルト入力パスワード６０を読み出して、空き状態にあるユーザ入力パスワード格納領域６５にユーザ入力パスワード６６として書き込む書込み処理７０を行う。

【００４６】

次にデフォルト入力パスワード６０の値が書き込まれたユーザ入力パスワード６６と書込読出パスワード６２を読み出して照合比較処理７２を実行する。この場合、ユーザ入力パスワード６６は、デフォルト入力パスワード６０の書込処理７０によって書込読出パスワード６２と同じ値となっており、照合一致が得られることで書込読出モードとなるアクセス許可７４が行われる。

【００４７】

図４は、デフォルト入力パスワード６０及び書込読出パスワード６２の値を初期化による「００００００００ｈ」とした場合を例にとっているが、ハードディスクドライブ４４がアクセス許可を確立して書込及びまたは読出アクセスが可能となった後は、上位インタフェースからのパスワード書替コマンドによってデフォルト入力パスワード６０及び書込読出パスワード６２、更には読出オンリーパスワード６４の値を別の値に書き替えることができる。このパスワードの書替えは、図３に示したコマンド処理部４６のパスワード書替部５４により行われる。

【００４８】

図５は、図３のパスワード書替部５４によるパスワード書替処理である。まず上位装置４２側より書込読出パスワード（アクセス保護パスワード）６２の書替コマンドを発行する。この書込読出パスワード６２の書替コマンドは、例えば「Ｃｈａｎｇｅ　Ｐａｓｓｗｏｒｄ０“０Ｆ１Ｅ２Ｄ３Ｃ”」となる。この書替コマンドにより、図４の書込読出パスワード６２の値「００００００００ｈ」は、

図６の書替え処理７６によって「０Ｆ１Ｅ２Ｄ３Ｃｈ」に書き替えられる。

【００４９】

このように書込読出パスワード６２を書き替えた場合には、ユーザのパスワード入力を必要としないアクセス許可を確立するため、デフォルト入力パスワード６０についても書込読出パスワード６２と同じ値に書き替える。このデフォルト入力パスワード６０の書替コマンドは例えば「Ｃｈａｎｇｅ　Ｄｅｆｏｕｌｔ　Ｐｓｗ“０Ｆ１Ｅ２Ｄ３Ｃ”」であり、書替み処理７８により図示のように書込読出パスワード６２と同じ値に書き替えられる。

【００５０】

尚、設定済みのデフォルト入力パスワードに併せてアクセス保護パスワードを書替えてもよい。

このようにデフォルト入力パスワード６０及びアクセス保護パスワードとしての書込読出パスワード６２を別の値に書き替えた後についても、ハードディスクドライブ４４が再度使用開始となれば、上位装置４２でユーザがパスワードを入力しなくとも、デフォルト入力パスワード６０の値を書込処理８０によりユーザ入力パスワード６６として書き込み、次にデフォルト入力パスワード６０を書き込んだユーザ入力パスワード６６と書込読出パスワード６２との照合比較処理８２を行い、この場合もパスワードは一致することから、書込読出アクセスのアクセス許可８４を確立する。

【００５１】

勿論、正しいパスワードを入力しない時にアクセスを禁止したい場合には、図４の初期化によるオール０となっているデフォルト入力パスワード６０と書込読出パスワード６２のいずれか一方を別の値に書き替えれば良く、デフォルト入力パスワード６０と書込読出パスワード６２が異なれば照合一致処理で不一致となることからアクセス許可は得られず、書込読出パスワード６２に一致するユーザのパスワード入力のみによってアクセス許可を確立することができる。

【００５２】

図６は、図３のパスワード検証部４８に設けたアクセスモード設定部５８で確立されるハードディスクドライブ４４のアクセスモードとアクセス内容である。

即ち、アクセスモードは書込読出モード、読出オンリーモード及びセキュリティモードの３つとなり、書込読出モードは通常の読出コマンドと書込コマンドを受け付ける。またデフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードの変更を許可する。

【００５３】

読出オンリーモードは、通常の読出コマンドのみを受け付ける。この場合にも、デフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードの変更を許可する。更にセキュリティモードは、通常の読出コマンドと書込コマンドによるアクセスは一切不可とするが、パスワード入力を伴う読出コマンドまたは書込コマンドは受け付ける。もちろん、パスワード照合一致が得られて初めて各コマンドに対するアクセス許可が行われる。

【００５４】

ここで図３の実施形態にあっては、ハードディスクドライブ４４の不揮発性メモリ４０にデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４を保存した場合であるが、本発明の他の実施形態として各パスワードを全て磁気ディスク媒体５２に格納しても良いし、ハードディスクドライブ４４の不揮発性メモリ４０と磁気ディスク媒体５２に分けて保存するようにしても良い。

【００５５】

図７は、本発明のハードディスクドライブ４４におけるパスワードの保存形態を表している。保存形態１は図３の実施形態であり、デフォルト入力パスワード及びアクセス保護用のパスワードは共にハードディスクドライブ４４側に格納している。保存形態２はデフォルト入力パスワード及びアクセス保護用のパスワードを全て磁気ディスク媒体５２に格納した場合である。

【００５６】

保存形態３はデフォルト入力パスワードをハードディスクドライブ４４側に格納し、アクセス保護用のパスワードについては磁気ディスク媒体５２側に格納した場合である。更に保存形態４はデフォルト入力パスワードを磁気ディスク媒体５２に保存し、アクセス保護用のパスワードはハードディスクドライブ４４に格

納した場合である。この保存形態２，３，４を具体的に説明すると、図８，図１０，図１１のようになる。

図８は図７の保存形態２であり、磁気ディスク媒体５２のパスワード格納領域６８にデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４を保存している。このためハードディスクドライブ４４の使用開始時には、パスワード検証部４８がアクセス実行部を経由して磁気ディスク媒体５２からデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４を読み出してワークメモリ３８のパスワード格納領域６７に展開する。またワークメモリ３８にはユーザ入力パスワード６６を格納するためのユーザ入力パスワード格納領域６５が確保されている。

【００５７】

図９は図８の磁気ディスク媒体５２のパスワード保存状態である。この実施形態にあっては、磁気ディスク媒体の論理ブロックアドレスＬＢＡ＝１が通常のリードコマンドまたはライトコマンドでアクセスすることのできないディスク管理領域７０に割り当てられていることから、ディスク管理領域７０の中の専用領域としてパスワード保存領域６８を確保し、ここにデフォルト入力パスワード６０、読出オンリーパスワード６４及び書込読出パスワード６２を保存している。

【００５８】

図１０は図７の保存形態３であり、ハードディスクドライブ４４側となる不揮発性メモリ４０に確保したパスワード格納領域４５にデフォルト入力パスワード６０を保存し、一方、磁気ディスク媒体５２のパスワード格納領域６８にはアクセス保護用の書込読出パスワード６２と読出オンリーパスワード６４を保存している。

【００５９】

このため、ワークメモリ３８にはパスワード格納領域６７が確保されており、ハードディスクドライブ４４の使用開始時にアクセス検証部４８はアクセス実行部５０を介して、まず磁気ディスク媒体５２のパスワード格納領域６８から読出オンリーパスワード６２及び読出オンリーパスワード６４を読み出してワークメモリ３８に展開する。もちろんワークメモリ３８には、ユーザ入力パスワード６

６を格納するためのユーザ入力パスワード格納領域６５も確保されている。

【００６０】

図１１は図７の管理モード４の実施形態であり、この実施形態にあっては、磁気ディスク媒体５２のパスワード格納領域６８にデフォルト入力パスワード６０を保存し、一方、ハードディスクドライブ４４の不揮発性メモリ４０に設けたパスワード保存領域４５にはアクセス保護用の書込読出パスワード６２と読出オンリーパスワード６４を保存している。

【００６１】

またワークメモリ３８にはパスワード格納領域６７が確保され、ハードディスクドライブ４４の使用開始時にアクセス検証部４８は、まずアクセス実行部５０を介して磁気ディスク媒体５２のパスワード格納領域６８からデフォルト入力パスワード６０を読み出して、ワークメモリ３８に図示のように展開する。

尚、図８，図１０及び図１１の保存形態２，３，４のそれぞれにおけるハードディスクドライブ４４に設けているコマンド処理部４６、パスワード検証部４８、アクセス実行部５０、パスワード書替部５４、パスワード照合部５６、アクセスモード設定部５８の処理機能は、図３の保存形態１の実施形態と同じである。

【００６２】

図１２は、ハードディスクドライブ４４を対象とした本発明のアクセス保護におけるユーザのパスワード入力を必要としないアクセス保護処理のフローチャートである。この処理を例えば図３の保存形態１の実施形態を例にとって説明すると次のようになる。

ハードディスクドライブ４４の電源投入、運用中におけるインタフェースのリセットコマンド、更には重大エラーからの内部リセット等を受けてハードディスクドライブ４４の使用が開始されると、まずステップＳ１でデフォルト入力パスワード６０を読み出してユーザ入力パスワード格納領域６５に書き込む設定処理を行う。続いてステップＳ２でデフォルト入力パスワード６０に書き替えられたユーザ入力パスワード６６と書込読出パスワード６２を比較照合する。

【００６３】

このとき図４のようにユーザ入力パスワード６６と書込読出パスワード６２が

同じ値であれば、ステップＳ３で照合一致が判別され、ステップＳ６で書込読出モードが確立される。一方、ステップＳ３でデフォルト入力パスワード６０で書き替えたユーザ入力パスワード６６が書込読出パスワード６２に不一致であった場合には、ステップＳ４で読出オンリーパスワード６４とデフォルト入力パスワード６０で書き替えられたユーザ入力パスワード６６の比較照合を行う。

【００６４】

この比較照合でステップＳ５で照合一致が判別されると、ステップＳ７で、この場合には読出オンリーモードが設定される。一方、ステップＳ５においても照合不一致となった場合には、ステップＳ８のセキュリティモードに進み、通常のリードコマンドあるいはライトコマンドによるアクセスは一切禁止し、ユーザのパスワード入力に伴うアクセスのみを受け付けることになる。

【００６５】

図１３は、ユーザがパスワードを入力した場合のアクセス保護処理のフローチャートである。このユーザがパスワードを入力した場合の処理は、図１２のステップＳ８でセキュリティモードに入った状態、あるいは装置使用開始時にユーザがパスワードを入力した場合、更には運用中の適宜のタイミングのいずれにおいても、ユーザによるパスワード入力があれば実行される処理となる。

【００６６】

まずユーザのパスワード入力に伴うパスワード転送コマンドを受信すると、ステップＳ１で、ユーザが入力したパスワードをワークメモリ３８のユーザ入力パスワード格納領域６５にユーザ入力パスワード６６として設定する。次にステップＳ２でユーザ入力パスワード６６と書込読出パスワード６２を比較照合する。

ステップＳ３で照合一致が得られれば、ステップＳ６の書込読出モードを設定する。不一致であれば、ステップＳ４で読出オンリーパスワードと比較照合し、ステップＳ５で照合一致が得られれば、ステップＳ７の読出オンリーモードを設定する。ステップＳ５でも照合不一致であった場合には、ステップＳ８のセキュリティモードを設定し、通常コマンドによるアクセスは一切禁止する。

【００６７】

図１４は、ハードディスクドライブ４４を対象とした本発明のアクセス保護の

他の実施形態のフローチャートであり、このフローチャートにあっては、必ずユーザによるパスワード入力操作を必要とする。図１４の処理を図３の保存形態１の実施形態を例にとって説明すると、次のようになる。

ハードディスクドライブ４４の電源投入等により装置の使用が開始されると、まずステップＳ１でデフォルト入力パスワード６０を読み出してユーザ入力パスワード領域６５にユーザ入力パスワード６６として設定する。続いてステップＳ２でユーザのパスワード入力を待つ。ユーザのパスワード入力操作の実行でパスワード転送コマンドが受信されると、ユーザのパスワード入力ありを判別してステップＳ３に進み、ユーザが入力したパスワードは空き文字列か否かチェックする。

【００６８】

ユーザが入力したパスワードに正常に文字列が格納されていた場合には、ステップＳ４に進み、ユーザが入力したパスワードをユーザ入力パスワード領域６５に上書きする。一方、ユーザが入力したパスワードが空き文字列であった場合には、ステップＳ４の上書きは行わず、ステップＳ１で書き込んだデフォルト入力パスワード６０の値をそのままユーザ入力パスワード６６として残す。

【００６９】

続いてステップＳ５でユーザ入力パスワード６６と書込読出パスワード６２を比較照合し、ステップＳ６で照合一致が得られれば、ステップＳ９で書込読出モードを設定する。照合不一致であれば、ステップＳ７でユーザ入力パスワード６６と読出オンリーパスワード６２を比較照合し、ステップＳ８で照合一致が得られれば、ステップＳ１０で読出オンリーモードを設定する。照合不一致であれば、ステップＳ１１でセキュリティモードを設定し、通常コマンドによるアクセスを禁止する。

【００７０】

この図１４の処理にあっては、ユーザがパスワードの文字列を入力せずにパスワード入力の実行操作のみを行った場合、ユーザが入力したパスワードの空き文字列を認識してユーザ入力パスワードの代わりにデフォルト入力パスワードを使用した比較照合が行われ、実質的にユーザはパスワードの文字列を必要とするこ

となく、ハードディスクドライブ４４のアクセス可能状態を確立することができる。

２．リムーバブル媒体の記憶装置

図１５は本発明が適用されるリムーバブル媒体を用いた記憶装置である光磁気ディスクドライブの回路ブロック図である。勿論、本実施形態は、リムーバブル磁気ディスクや相変化型光ディスク等の可換記憶装置にそのまま適用できる。光ディスクドライブは、コントロールボード１１０とエンクロージャ１１１で構成される。

【００７１】

コントロールボード１１０には光磁気ディスクドライブの全体的な制御を行うＭＣＵ１２、ワークメモリとなるＲＡＭ１０６、不揮発性メモリとなるフラッシュＲＯＭ１０８、上位装置との間でコマンド及びデータのやり取りを行うインタフェース１１７、光ディスク媒体に対するデータのリード・ライトに必要な処理を行う光磁気ディスクコントローラ（ＯＤＣ）１１４、ＤＳＰ１１６、及びバッファメモリ１１８が設けられる。

【００７２】

光磁気ディスクコントローラ１１４には、フォーマッタ１１４－１とＥＣＣ処理ユニット１１４－１が設けられる。ライトアクセス時には、フォーマッタ１１４－１がＮＲＺライトデータを媒体のセクタ単位に分割して記録フォーマットを生成し、ＥＣＣ処理ユニット１１４－１がセクタライトデータ単位にＥＣＣコードを生成して付加し、更に必要ならばＣＲＣコードを生成して付加する。

【００７３】

更に、ＥＣＣエンコードの済んだセクタデータを例えば１－７ＲＬＬ符号に変換する。リードアクセス時には、復調されたセクタリードデータを１－７ＲＬＬ符号から逆変換し、ＥＣＣ処理ユニット１１４－２でＣＲＣチェックした後にエラー検出訂正し、更にフォーマッタ１１４－１でセクタ単位のＮＲＺデータを連結してＮＲＺリードデータのストリームとし、上位装置に転送させる。

【００７４】

光ディスクコントローラ１１４に対してはライトＬＳＩ回路１２０が設けられ、ライトＬＳＩ回路１２０にはライト変調ユニット１２１とレーザダイオード制御回路１２２が設けられる。レーザダイオード制御回路１２２の制御出力は、エンクロージャ１１１側に設けたレーザダイオードユニット１３０に与えられている。レーザダイオードユニット３０はレーザダイオード１３０－１とモニタ用ディテクタ１３０－２を一体に備える。ライト変調ユニット１２１は、ライトデータをＰＰＭ記録またはＰＷＭ記録のでデータ形式に変換する。

【００７５】

レーザダイオードユニット１３０を使用して記録再生を行うリムーバブル媒体として光磁気記憶媒体を使用する。媒体の記録フォーマットはゾーンＣＡＶである。更に、媒体の記録方式は、媒体上のマークの有無に対応してデータを記録するピットポジション記録（ＰＰＭ記録）、又はマークのエッジ即ち前縁と後縁をデータに対応させるパルス幅記録（ＰＷＭ記録）を採用している。

【００７６】

光ディスクドライブにＭＯカートリッジ媒体をローディングした際には、まず媒体のＩＤ部をリードし、そのピット間隔からＭＣＵ１１２において媒体の種別を認識し、種別結果をライトＬＳＩ回路１２０に通知する。

光ディスクドライブ１１４からのセクタライトデータは、ライト変調ユニット１２１でＰＷＭ記録データに変換される。そしてライト変調ユニット１２１で変換されたＰＷＭ記録データは、レーザダイオード制御ユニット１２２に与えられ、レーザダイオード１３０－１の発光駆動で媒体に書き込まれる。

【００７７】

光ディスクドライブ１１４に対するリード系統としては、リードＬＳＩ回路１２４が設けられ、リードＬＳＩ回路１２４にはリード復調ユニット１２５と周波数シンセサイザ１２６が内蔵される。リードＬＳＩ回路１２４に対してはＩＤ／ＭＯ用ディテクタ１３２からレーサビームの媒体戻り光の受光信号が、ヘッドアンプ３４を介してＩＤ信号及びＭＯ信号として入力されている。

【００７８】

リードＬＳＩ回路１２４のリード復調ユニット１２５には、ＡＧＣ回路、フィ

ルタ、セクタマーク検出回路等の回路機能が設けられ、入力したＩＤ信号及びＭＯ信号よりリードクロックとリードデータを作成し、ＰＷＭ記録データを元のＮＲＺデータに復調している。

またスピンドルモータ４０の制御としてゾーンＣＡＶを採用していることから、ＭＣＵ１１２からリードＬＳＩ回路１２４に内蔵した周波数シンセサイザ１２６に対しゾーン対応のクロック周波数を発生させるための分周比の設定制御が行われている。周波数シンセサイザ１２６はプログラマブル分周器を備えたＰＬＬ回路であり、媒体のゾーン位置に応じて予め定めた固有の周波数をもつ基準クロックをリードクロックとして発生する。

【００７９】

リードＬＳＩ１２４で復調されたリードデータは、光ディスクコントローラ１１４に与えられ、１－７ＲＬＬ符号の逆変換後にＥＣＣ処理ユニット１１４－２のエンコード機能によってＣＲＤチェックとＥＣＣ処理を受けてＮＲＺセクタデータが復元され、フォーマッタ１１４－１でＮＲＺリードデータのストリームに繋げた後に、バッファメモリ１１８を経由して上位インタフェース１１７により上位装置に転送される。

【００８０】

ＭＣＵ１１２に対しては、ＤＳＰ１１６を経由してエンクロージャ１１１側に設けた温度センサ１３６の検出信号が与えられ、装置内部の環境温度に基づき、レーザダイオード制御ユニット１２２におけるリード、ライト、イレーズの各発光パワーを最適値に制御する。

ＭＣＵ１１２は、ＤＳＰ１１６を経由してドライバ１３８によりスピンドルモータ４０を制御し、例えば６０００ｒｐｍの一定速度で回転させる。またＭＣＵ１１２は、ＤＳＰ１６からドライバ１４２を介してエンクロージャ１１１側に設けた電磁石に通電し媒体に記録磁場を与える。

【００８１】

ＤＳＰ１１６は、媒体に対しレーザダイオード１３０からのビームの位置決めを行うためのサーボ機能を備え、目的トラックにシークしてオントラックするためのシーク制御を行う。このシーク制御は、ＭＣＵ１１２による上位コマンドに

対するライトアクセス又はリードアクセスに並行して同時に実行することができる。

【００８２】

ＤＳＰ１１６のサーボ機能を実現するため、エンクロージャ１１１側の光学ユニットに媒体からのビーム戻り光を受光するＦＥＳ用ディテクタ１４５を設け、ＦＥＳ検出回路（フォーカスエラー信号検出回路）１４６が、ＦＥＳ用ディテクタ４５の受光出力からフォーカスエラー信号Ｅ１を作成してＤＳＰ１１６に入力している。

【００８３】

またエンクロージャ１１１側の光学ユニットに媒体からのビーム戻り光を受光するＴＥＳ用ディテクタ１４７を設け、ＴＥＳ検出回路（トラッキングエラー信号検出回路）１４８がＴＥＳ用ディテクタ４７の受光出力からトラッキングエラー信号Ｅ２を作成し、ＤＳＰ１１６に入力している。トラッキングエラー信号Ｅ２はＴＺＣ検出回路（トラックゼロクロス検出回路）１５０に入力され、トラックゼロクロスパルスＥ３を作成してＤＳＰ１１５に入力している。

【００８４】

エンクロージャ１１１側には、媒体に対しレーザビームを照射する対物レンズのレンズ位置を検出するレンズ位置センサ１５２が設けられ、そのレンズ位置検出信号（ＬＰＯＳ）Ｅ４をＤＳＰ１１６に入力している。更にＤＳＰ１１６は、媒体上のビームスポットの位置を制御するため、ドライバ１５８，１６２，１６６を介してフォーカスアクチュエータ１６０、レンズアクチュエータ１６４及びＶＣＭ１６８を制御駆動している。

【００８５】

ここで光ディスクドライブにおけるエンクロージャ１１の概略は図１６のようになる。ハウジング１６７内にはスピンドルモータ１４０が設けられ、スピンドルモータ１４０の回転軸のハブに対しインレットドア１６９側よりＭＯカートリッジ１７０を挿入することで、内部のＭＯ媒体１７２がスピンドルモータ１４０の回転軸のハブに装着されるローディングが行われる。

【００８６】

ローディングされたＭＯカートリッジ１７０のＭＯ媒体１７２の下側には、ＶＣＭ１６８により媒体トラックを横切る方向に移動自在なキャリッジ１７６が設けられている。キャリッジ１７６上には対物レンズ１８０が搭載され、固定光学系１７８に設けているレーザダイオードからのビームをプリズム１８２を介して入射し、ＭＯ媒体１７２の媒体面にビームスポットを結像している。

【００８７】

対物レンズ１８０は図１５のエンクロージャ１１１に設けたフォーカスアクチュエータ１６０により光軸方向に移動制御され、またレンズアクチュエータ１６４により媒体トラックを横切る半径方向に例えば数十トラックの範囲内で移動することができる。

図１７は、図１５の光ディスクドライブを対象とした本発明のデフォルト入力パスワードを用いたアクセス保護の実施形態であり、この実施形態にあっては、図７の保存形態２に従ってデフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードを記憶媒体に保存したことを特徴とする。

【００８８】

図１７において、ＭＯ媒体１７２の通常コマンドでは読み出し不可の領域にはパスワード格納領域１８２が設けられ、ここにデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４を格納している。またワークメモリ１０６にはユーザ入力パスワード格納領域２０２が設けられ、ここにユーザ入力パスワード６６を格納している。

【００８９】

光ディスクドライブ９０にＭＯカートリッジ１７０を挿入すると、ワークメモリ１６０のパスワード格納領域２００に図示のようにデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４が読み出され、コマンド処理部９２、パスワード検証部９４及びアクセス実行部９６によるアクセス保護処理を受けることになる。

【００９０】

デフォルト入力パスワードを用いたアクセス保護のため光ディスクドライブ９０には、コマンド処理部９２、パスワード検証部９４及びアクセス実行部９６が

設けられる。パスワード検証部９４はパスワード照合部１００、アクセスモード設定部１０２を備える。またコマンド処理部９２にはパスワード書替部９８が設けられている。

【００９１】

このようなドライブ側の構成は、例えばハードディスクドライブを対象とした図３の実施形態と基本的に同じであるが、更にリムーバブル媒体としてＭＯ媒体１７２を備えたＭＯカートリッジ１７０を使用する光ディスクドライブ９０にあっては、パスワード検証部９４に新たに有効期限管理部１０４を設けている。

有効期限管理部１０４は、デフォルト入力パスワード６０が有効に使用される期限を管理しており、ＭＯ媒体１７２もしくは光ディスクドライブ９０に予め設定した有効期限が切れると、デフォルト入力パスワード６０を異なる値に強制的に書き替え。

【００９２】

このため、有効期間にあってはデフォルト入力パスワード６０が書込読出パスワード６２と同じであっても、有効期限が切れると書込読出パスワード６２とは別の例えば１６進値「３Ｆ２３１２００」とのＥＸ－ＯＲをとった値に変ってしまうため、パスワードの入力を行わない光ディスクドライブ９０のアクセスは禁止されることになる。

【００９３】

また逆に一定期間経過した時に、デフォルト入力パスワード６０を、ある規則で書替えるように実装し、この規則で書替えを行ったときに、アクセス保護パスワードである例えば書込読出パスワード６２と等しくなるような値を書替値として設定しておく。こうすれば一定期間経過した時に、パスワードを入力しなくともアクセスできるような使い方ができる。

【００９４】

図１８は、図１７の光ディスクドライブ９０におけるユーザのパスワード入力を必要としないアクセス保護の処理動作である。媒体メーカから出荷された時点でＭＯディスク１７２は初期化処理されており、デフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４は、ＭＯカートリッ

ジ１７０を初期化した際の初期値である１６進の「ＣＦ２３ＣＦ２３ｈ」が格納されている。

【００９５】

このため、初期化されたパスワードの保存状態で光ディスクドライブの使用を開始すると、まずデフォルト入力パスワード６０が読み出され、書込み処理１８４によってユーザ入力パスワード６６としてユーザ入力パスワード格納領域２０２に書き込まれる。

続いてデフォルト入力パスワード６０の書込みを受けたユーザ入力パスワード６６と書込読出パスワード６２の照合比較処理１８６を行い、照合一致が得られることでアクセス許可１８８、即ち書込読出モードの設定が行われる。このため、図１７の光ディスクドライブ９０にあっても、ユーザはパスワード入力を必要とすることなく、ＭＯカートリッジ１７０のアクセス許可状態を確立することができる。

【００９６】

図１９は、図１８のようなデフォルト入力パスワードに基づくアクセス許可が確立された書込読出モードの状態で、パスワード書替えを行った場合である。このパスワード書替えにあっては、図１８のデフォルト入力パスワード６０の初期値「ＣＦ２３ＣＦ２３ｈ」をパスワード書替コマンド１９０に基づく書替処理１９２によって別の値「ＡＢ８９ＡＢ８９ｈ」に書き替えている。

【００９７】

このようにデフォルト入力パスワード６０を別の値に書き替えてしまうと、次に光ディスクドライブ９０の使用を開始したときユーザがパスワードを入力しないと、まず書込え処理１９４によってユーザ入力パスワード６６が変更後のデフォルト入力パスワード６０の値「ＡＢ８９ＡＢ８９ｈ」に書き替えられ、次に書込読出パスワード６２の値「ＣＦ２３ＣＦ２３ｈ」との照合比較処理１９６が行われ、この場合は照合不一致となってアクセス禁止１９８、即ちセキュリティモードが設定されてしまう。

【００９８】

この図１９のようなデフォルト入力パスワード６０の書替えは、次のような場

合に有効である。まず光ディスクドライブ９０の本来の使用者Ａ氏は、図１８のようにデフォルト入力パスワード６０及び書込読出パスワード６２を同じ初期値「ＣＦ２３ＣＦ２３ｈ」とした状態で秘書のＢ氏に処理を依頼する。依頼を受けたＢ氏は、パスワードを知らなくとも電源を投入することでデフォルト入力パスワード６０に基づくアクセス許可による読出書込モードが確立され、光ディスクドライブ９０を使用した処理を行うことができる。

【００９９】

ここで本来の使用者であるＡ氏は仕事を依頼したＢ氏に対し、仕事を終了したならばパスワード書替コマンド「Ｃｈａｎｇｅ　Ｄｅｆｏｕｌｔ　Ｐｓｗ“ＡＢ８９ＡＢ８９”」を入力するように依頼しておく。そこで、依頼を受けたＢ氏は、業務が終了したならばＡ氏から指示されたコマンドを入力する。

このコマンドを入力すると、図１９のように、デフォルト入力パスワード６０は「ＡＢ８９ＡＢ８９ｈ」に書き替えられてしまう。

【０１００】

このため本来の使用者Ａ氏より依頼を受けて業務を行ったＢ氏が、業務を終了してデフォルト入力パスワード６０を書き替えてＭＯカートリッジ１７０のイジェクト操作を行うと、このイジェクト操作に伴う指示を受けて、ワークメモリ１６０に展開しているデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４は、ＭＯカートリッジ１７０のパスワード格納領域１８２にライトバックされた後にＭＯカートリッジ１７０が排出される。

【０１０１】

このため、ＭＯカートリッジ１７０が排出された後は、再度、ＭＯカートリッジ１７０を光ディスクドライブ９０に挿入しても、このときワークメモリ１０６に読み出されるデフォルト入力パスワード６０は、図１９のように書込読出パスワード６２とは異なった値に変更されており、書込読出パスワード６０の値をパスワードとして入力しない限り、ＭＯカートリッジ１７０のアクセスは一切禁止することができる。

【０１０２】

即ち本来の使用者Ａ氏は、Ｂ氏に業務が終了したらデフォルト入力パスワード

書替コマンドの入力を指示しておくことで、Ｂ氏が作業を終了した後に、第３者は勿論のことＢ氏がＡ氏の光ディスクドライブ９０を使用するために電源を投入しても、本来の使用者であるＡ氏しか分かっていないパスワード「ＣＦ２３ＣＦ２３ｈ」を入力しない限り、光ディスクドライブ９０はセキュリティモードとなってアクセスを一切禁止することができる。

【０１０３】

図２０は、図７の保存形態１に対応した光ディスクドライブ９０の実施形態であり、この実施形態にあっては、デフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードをドライブ本体側に保存したことを特徴とする。

図２０において、光ディスクドライブ９０の不揮発性メモリ１０８にはパスワード格納領域２００が設けられ、ここにデフォルト入力パスワード６０、書込読出パスワード６２及び読出オンリーパスワード６４を格納している。またワークメモリ１０６にはユーザ入力パスワード格納領域２０２が設けられ、ここにユーザ入力パスワード６６を格納している。

【０１０４】

デフォルト入力パスワードを用いたアクセス保護のため光ディスクドライブ９０には、コマンド処理部９２、パスワード検証部９４及びアクセス実行部９６が設けられる。パスワード検証部９４はパスワード照合部１００、アクセスモード設定部１０２を備える。またコマンド処理部９２にはパスワード書替部９８が設けられている。更にパスワード検証部９４に新たに有効期限管理部１０４を設けている。

【０１０５】

図２１は、図７の保存形態３に対応した光ディスクドライブ９０の実施形態であり、この実施形態にあっては光ディスクドライブ９０の不揮発性メモリ１０８のパスワード格納領域２００にデフォルト入力パスワード６０を保存し、一方、書込読出パスワード６２及び読出オンリーパスワード６４についてはリムーバブル媒体であるＭＯカートリッジ１７０のパスワード格納領域１８２に保存したことを特徴とする。

【０１０６】

このため、ＭＯカートリッジ１７０を光ディスクドライブ９０に挿入した場合には、パスワード検証部９４はアクセス実行部９６を介して、まずＭＯカートリッジ１７０のパスワード格納領域１８２から書込読出パスワード６２と読出オンリーパスワード６４を読み出してワークメモリ１０６に展開する。

図２２は、図７の保存形態４を適用した光ディスクドライブ９０の実施形態であり、保存形態４にあっては光ディスクドライブ９０の不揮発性メモリ１０８のパスワード格納領域２００にアクセス保護用の書込読出パスワード６２及び読出オンリーパスワード６４を保存し、一方、デフォルト入力パスワード６０はＭＯカートリッジ１７０のパスワード格納領域１８２に保存している。

【０１０７】

このため、ＭＯカートリッジ１７０を光ディスクドライブ９０に挿入した場合には、パスワード検証部９４はアクセス実行部９６を介してＭＯカートリッジ１７０からデフォルト入力パスワード６０を読み出し、ワークメモリ１６０のパスワード格納領域２０４に図示のように展開する。

図２３は、光ディスクドライブ９０におけるユーザがパスワードを入力しなかった場合のアクセス保護処理のフローチャートであり、図１７の保存形態２の場合を例にとって説明すると次のようになる。

【０１０８】

光ディスクドライブ９０にＭＯカートリッジ１７０を挿入すると、ステップＳ１でデフォルト入力パスワード６０を読み出してユーザ入力パスワード領域にユーザ入力パスワード６６として書込み設定する。続いてステップＳ２で、ユーザ入力パスワード６６と書込読出パスワード６２を比較照合し、ステップＳ３で照合一致が得られると、ステップＳ６の書込読出モードを設定する。

【０１０９】

照合不一致であれば、ステップＳ４でユーザ入力パスワード６６と読出オンリーパスワード６４を比較照合し、ステップＳ５で照合一致が得られれば、ステップＳ７で読出オンリーモードを設定する。照合不一致であれば、ステップＳ８でセキュリティモードとし、パスワードを伴わないアクセスは一切禁止とする。このステップＳ６，Ｓ７で書込読出モードあるいは読出モードが設定されると、ス

テップＳ９でパスワード検証部９４に設けた有効期限管理部１０４による期限管理処理が行われる。

【０１１０】

図２４は、図２３のステップＳ９の期限管理処理の一実施形態のフローチャートである。この期限管理処理にあっては、まずステップＳ１でデフォルト入力パスワードの初期化あるいはコマンドによる変更の有無をチェックし、初期化または変更があれば、ステップＳ２でカウンタＤＰＣをＤＰＣ＝０にセットし、ステップＳ３でカウンタＤＰＣを１つインクリメントする。

【０１１１】

もちろん、デフォルト入力パスワードの初期化あるいは変更がなければ、ステップＳ２をスキップして、ステップＳ３でカウンタＤＰＣを１つインクリメントする。続いてステップＳ４で、カウンタＤＰＣは予め定めた有効期限を与える規定値ＮＸＸ以上か否かチェックする。

カウンタＤＰＣの値が規定値ＮＸＸ未満であればステップＳ５をスキップするが、カウンタＤＰＣが規定値ＮＸＸ以上となった場合はステップＳ５に進み、光ディスクドライブ９０内で乱数列ＲＸを発生し、デフォルト入力パスワードの値ＰＤと乱数列ＲＸとの排他論理和を求め、これを新たなデフォルト入力パスワードの値とする。

【０１１２】

即ち、この実施形態にあっては、カウンタＤＰＣによって光ディスクドライブ９０の使用回数を計数しており、使用回数が規定値ＮＸＸに達すると、乱数列を使用して強制的にデフォルト入力パスワードをユーザの知り得ない値に変更し、有効期限以降のパスワードを入力しないアクセス許可を禁止する。

図２５は、図２のデフォルト入力パスワードの期限管理処理の他の実施形態のフローチャートである。この期限管理処理にあっては、ステップＳ１でデフォルト入力パスワードの初期化あるいは変更の有無をチェックしており、初期化または変更があれば、ステップＳ２でカウンタＤＰＣに所定の有効期限の時刻をセットする。続いてステップＳ３で、現在時刻がカウンタＤＰＣにセットした有効期限の時刻以降か否かチェックする。

【０１１３】

現在時刻がカウンタＤＰＣの有効期限の時刻以降であった場合には、ステップＳ５に進み、図２３の場合と同様、光ディスクドライブ９０内で乱数列ＲＸを発生して、そのときのデフォルト入力パスワードの値ＤＰとの排他論理和で置き換え、デフォルト入力パスワードの値を異なる値に強制的に変更し、有効期限以降でのパスワードの入力によらない光ディスクドライブ９０のアクセスを一切禁止する。

【０１１４】

また現在時刻がカウンタＤＰＣの有効期限の時刻以降となってステップＳ５に進んだ場合、デォルト入力パスワード６０をアクセス保護パスワード例えば書込読出パスワード６２と等しい値に変更することで、一定期間経過した時に、パスワードを入力しなくともアクセスできるような使い方が設定できる。

ここで光ディスクドライブ９０にあっては、図２３のフローチャートでユーザがパスワードを入力した場合の処理を例にとっているが、ユーザがパスワードを入力した場合の処理については、ハードディスクドライブにおける図１３のフローチャートと同じである。またユーザに必ずパスワード入力操作の実行を行わせるハードディスクドライブの図１４のフローチャートの処理についても、そのまま光ディスクドライブ９０に適用することができる。

【０１１５】

尚、上記の実施形態は、記憶装置としてハードディスクドライブ、光ディスクドライブを例にとるものであったが、これ以外に磁気テープドライブ、フロッピディスクドライブを含むことはもちろんである。また本発明は記憶装置に限定されず、パスワードによるアクセス保護を行う装置やシステム一般につきそのまま適用することができる。

【０１１６】

【発明の効果】

以上説明してきたように本発明によれば、パスワードを用いて保護する装置側例えば記憶装置側にデフォルト入力パスワードを格納し、ユーザからのパスワー

ド入力がない場合にはデフォルト入力パスワードをユーザ入力パスワードとみなしてパスワードの検証を行うため、デフォルト入力パスワードとアクセス保護用パスワードを同じ値にしておくことによって、ユーザがパスワード入力を行わなくともアクセス保護を解除して通常コマンドによるアクセスができ、ユーザによるパスワード入力を大幅に省略することができる。

【０１１７】

また記憶装置において既にアクセスが許可されている場合には、デフォルト入力パスワードのユーザによる書替えを可能とすることで、ユーザは必要に応じてパスワード入力を必要としないアクセス保護とパスワード入力を必要とするアクセス保護を使い分けることができる。

更にデフォルト入力パスワードの有効期限を管理し、期限を過ぎた場合にはデフォルト入力パスワードをユーザが知り得ない別な値に強制的に変更してしまうことで、パスワードの入力を省略した記憶装置のアクセス可能な状態を一定期間だけ限定的に継続させることができ、パスワード入力を省略できるという無防備な状態が長期間に亘って継続することを未然に防止できる。

【図面の簡単な説明】

【図１】

本発明の原理説明図

【図２】

本発明が適用されるハードディスクドライブのブロック図

【図３】

パスワードをドライブ本体に保存した本発明の実施形態の機能ブロック図

【図４】

ユーザのパスワード入力がない場合のデフォルト入力パスワードでアクセス許可を獲得するアクセス保護処理の説明図

【図５】

デフォルト入力パスワード及びアクセス制御用パスワードのコマンド書替処理の説明図

【図６】

本発明におけるアクセス種別の説明図

【図７】

本発明におけるパスワードの保存形態の説明図

【図８】

パスワードを媒体のみに保存した本発明の実施形態の機能ブロック図

【図９】

図８の媒体内のパスワード保存領域の説明図

【図１０】

パスワードをドライブ本体と媒体に分けて保存した本発明の実施形態の機能ブロック図

【図１１】

パスワードをドライブ本体と媒体に分けて保存した本発明の他の実施形態の機能ブロック図

【図１２】

ユーザのパスワード入力がない場合のアクセス保護処理のフローチャート

【図１３】

ユーザがパスワードを入力した場合のアクセス保護処理のフローチャート

【図１４】

ユーザがパスワード入力操作を必ず必要とするアクセス保護処理のフローチャート

【図１５】

本発明が適用される光ディスクドライブのブロック図

【図１６】

ＭＯカートリッジをローディングした装置内部構造の説明図

【図１７】

パスワードをリムーバブル媒体のみに保存した本発明の実施形態の機能ブロック図

【図１８】

ＭＯドライブに対しユーザのパスワード入力がなくデフォルト入力パスワードでアクセス許可を獲得するアクセス保護処理の説明図

【図１９】

デフォルト入力パスワードによるアクセスを禁止するためのパスワード書替処理の説明図

【図２０】

パスワードをＭＯドライブ本体に保存した本発明の実施形態の機能ブロック図

【図２１】

パスワードをＭＯドライブ本体とリムーバブル媒体に分けて保存した本発明の実施形態の機能ブロック図

【図２２】

パスワードをＭＯドライブ本体とリムーバブル媒体に分けて保存した本発明の他の実施形態の機能ブロック図

【図２３】

ＭＯドライブにおけるユーザのパスワード入力がない場合のアクセス保護処理のフローチャート

【図２４】

カウンタで使用回数を計数してデフォルト入力パスワードの期限を管理する図２２の有効期限管理処理のフローチャート

【図２５】

デフォルト入力パスワードの期限となる時刻を設定して管理する図２２の有効期限管理処理のフローチャート

【符号の説明】

１０，１１１：エンクロージャ

１２，１１０：コントロールボード

２２，１１２：メインコントロールユニット（ＭＣＵ）

３８，１０６：ワークメモリ（ＲＡＭ）

４０，１０８：不揮発性メモリ（フラッシュＲＯＭ）

４２：上位装置

４４：ハードディスクドライブ（ＨＤＤ）

４６，９２：コマンド処理部

４８，９４：パスワード検証部

５０，９６：アクセス実行部

５２：磁気ディスク媒体

５４，９８：パスワード書替部

５６，１００：パスワード照合部

５８，１０２：アクセスモード設定部

６０：デフォルト入力パスワード（ＤＰＷ）

６２：書込読出パスワード（アクセス保護用パスワード）

６４：書込オンリーパスワード（アクセス保護用パスワード）

６５：ユーザ入力パスワード領域

６６：ユーザ入力パスワード（ＵＰＷ）

６７：パスワード格納領域

６８：パスワード保存領域

７０：ディスク管理領域

９０：光ディスクドライブ（ＯＤＤ）

１０２：有効期限管理部

１７０：ＭＯカートリッジ（光磁気ディスクカートリッジ）

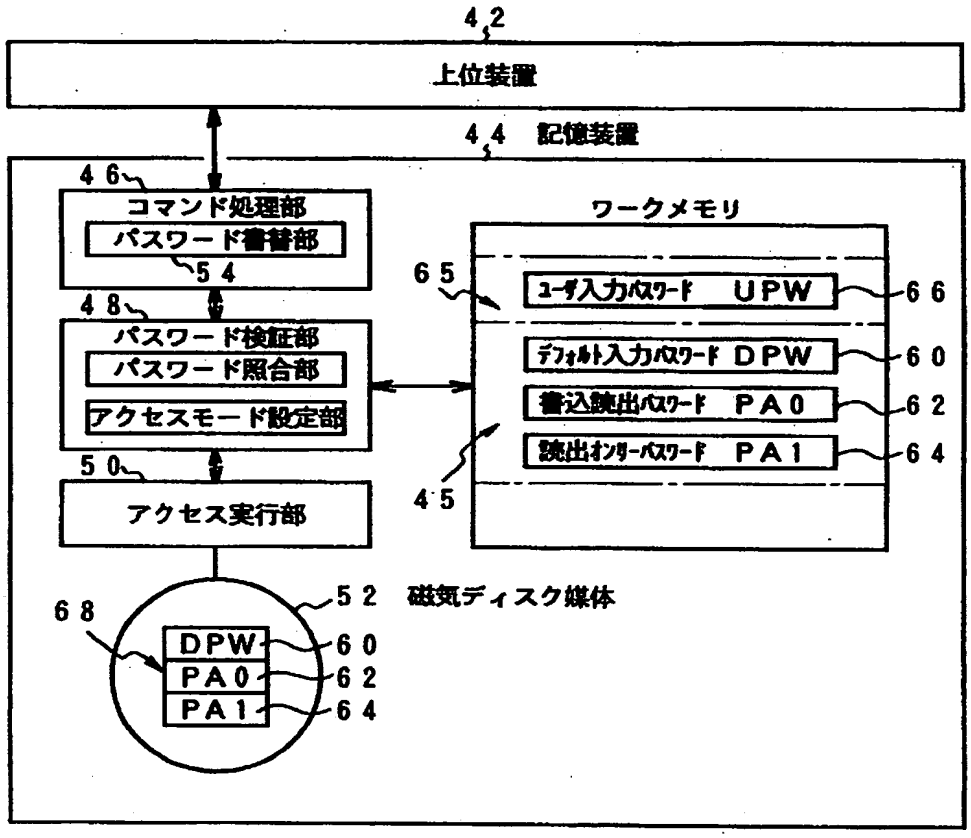
１７２：ＭＯ媒体（光磁気ディスク媒体）

【書類名】　　図面

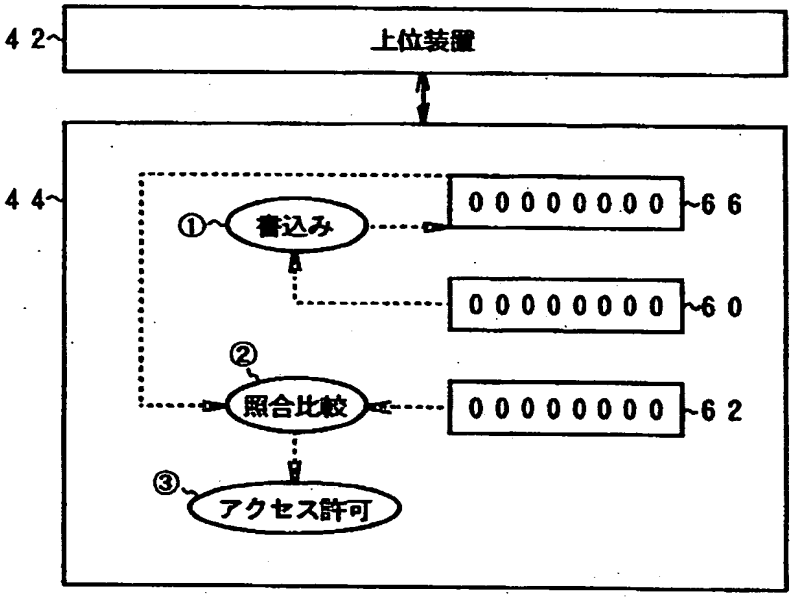
【図１】

本発明の原理説明図

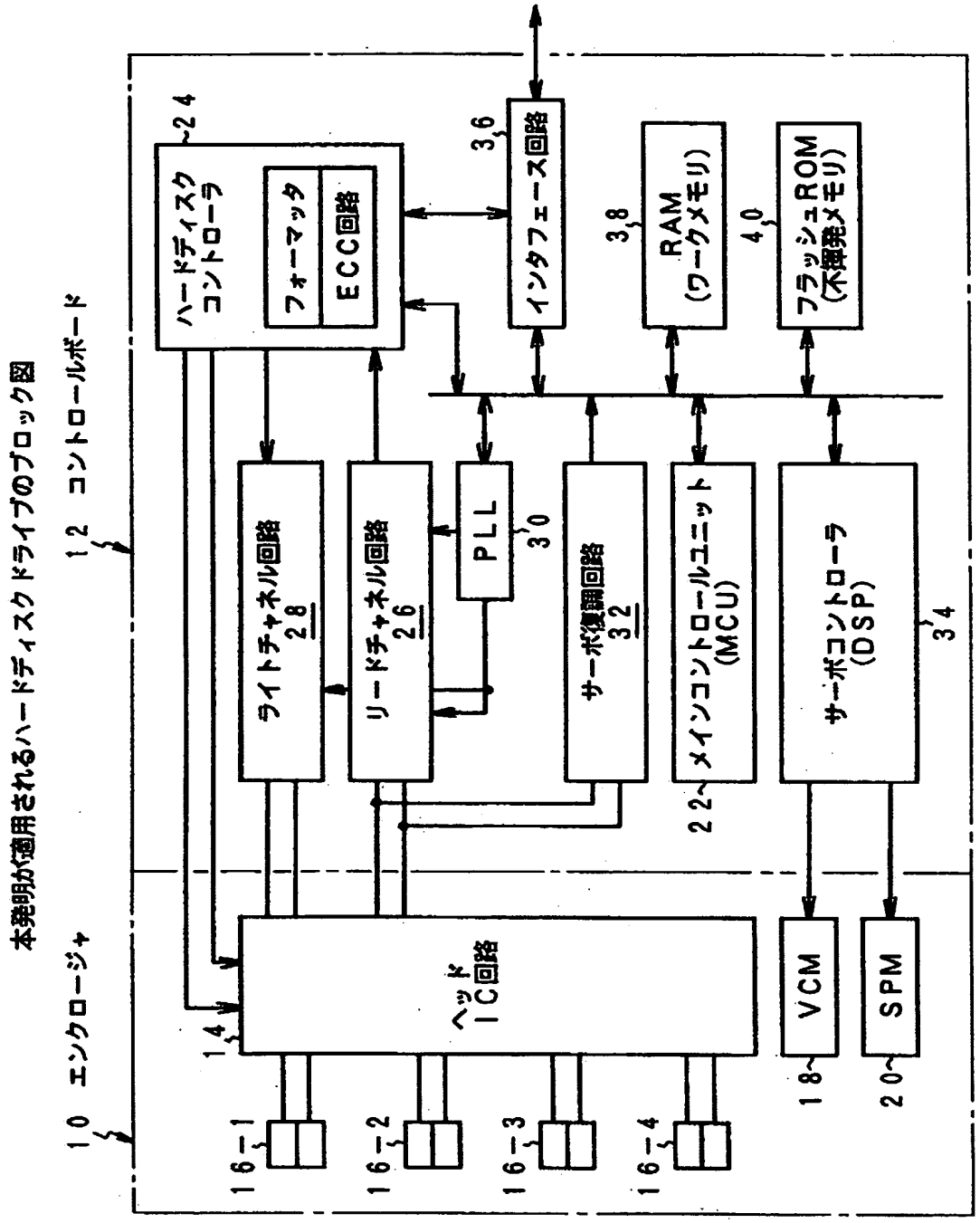
(A)



(B)

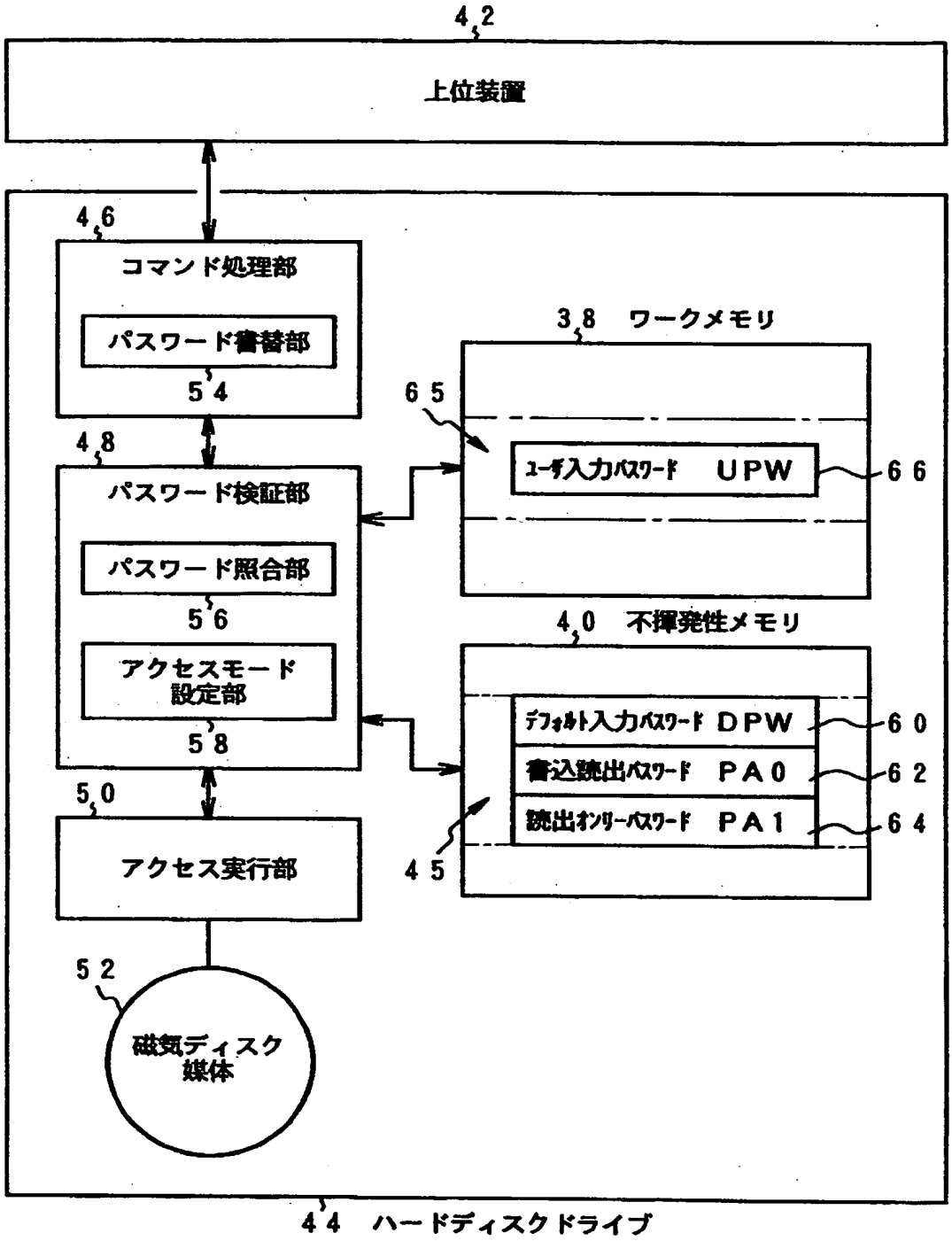


【図２】


本発明が適用されるハードディスクドライブのブロック図
10 エンクロージャ
12 コントロールボード
24 ハードディスクコントローラ
フォーマッタ
ECC回路
36 インタフェース回路
38 RAM (ワークメモリ)
40 フラッシュROM (不揮発メモリ)
28 ライトチャネル回路
26 リードチャネル回路
PLL 30
サーボ復調回路 32
22 メインコントロールユニット (MCU)
サーボコントローラ (DSP) 34
14 ヘッドIC回路
16-1
16-2
16-3
16-4
18 VCM
20 SPM

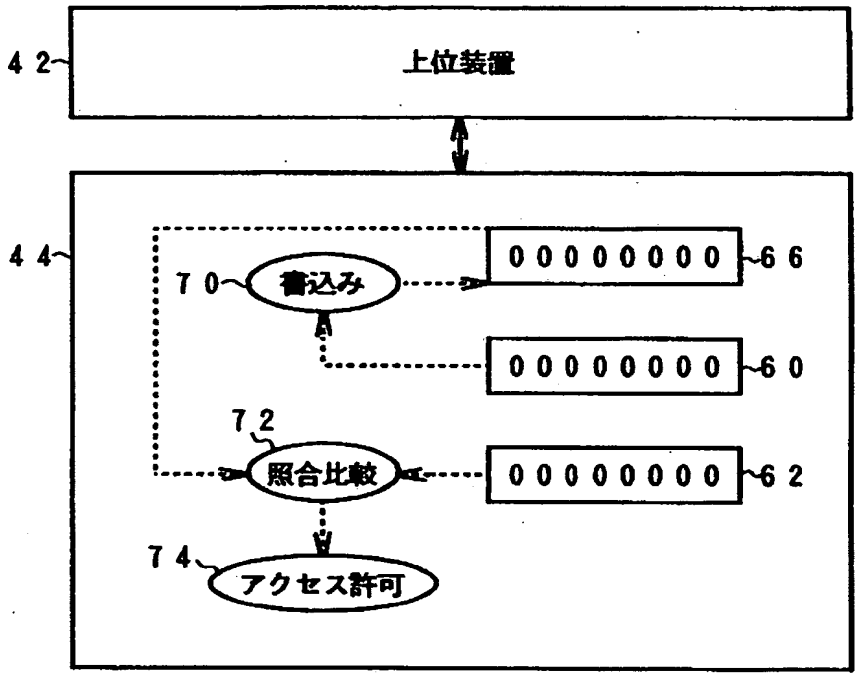
【図３】

パスワードをドライブ本体に保存した本発明の実施形態の機能ブロック図



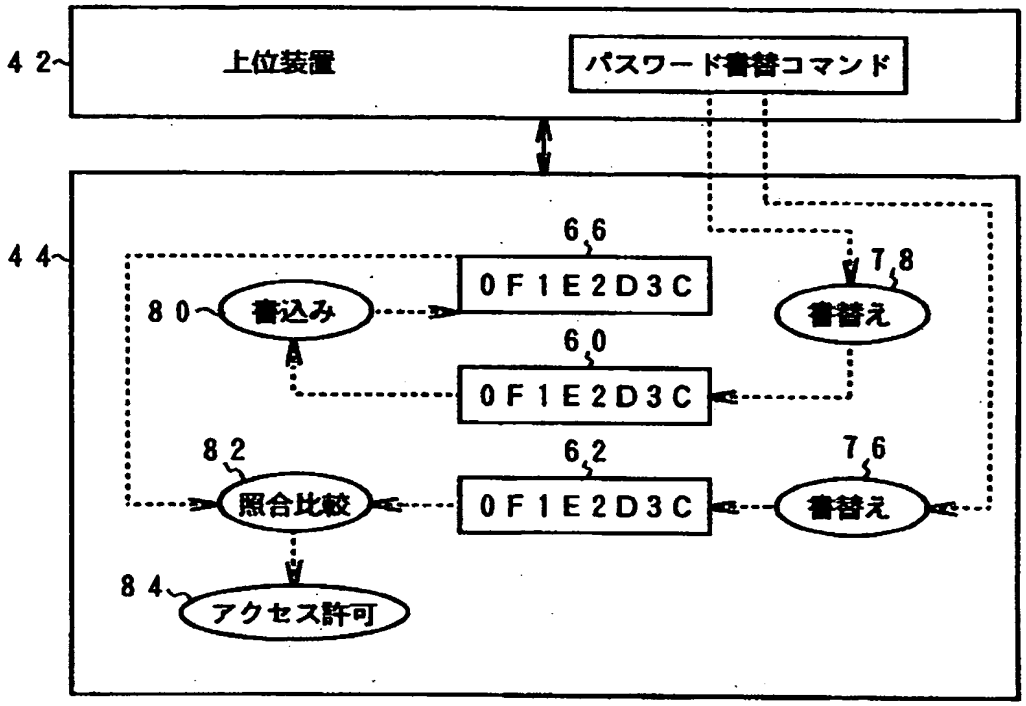
【図４】

ユーザのパスワード入力がない場合のデフォルト入力パスワードでアクセス許可を獲得するアクセス保護処理の説明図



【図５】

デフォルト入力パスワード及びアクセス制御用パスワードのコマンド書替処理の説明図



【図６】

本発明におけるアクセス種別の説明図

モード	アクセス内容
書込読出モード	通常の読出コマンドと書込コマンドを受け付ける。 デフォルト入力、読出、及び読出書込の各パスワードの変更を許可する。
読出オンリーモード	通常の読出コマンドのみを受け付ける。 デフォルト入力、読出、及び読出書込の各パスワードの変更を許可する。
セキュリティモード	アクセス不可とする。 パスワード入力を伴う読出コマンド又は書込コマンドのみを受け付ける。

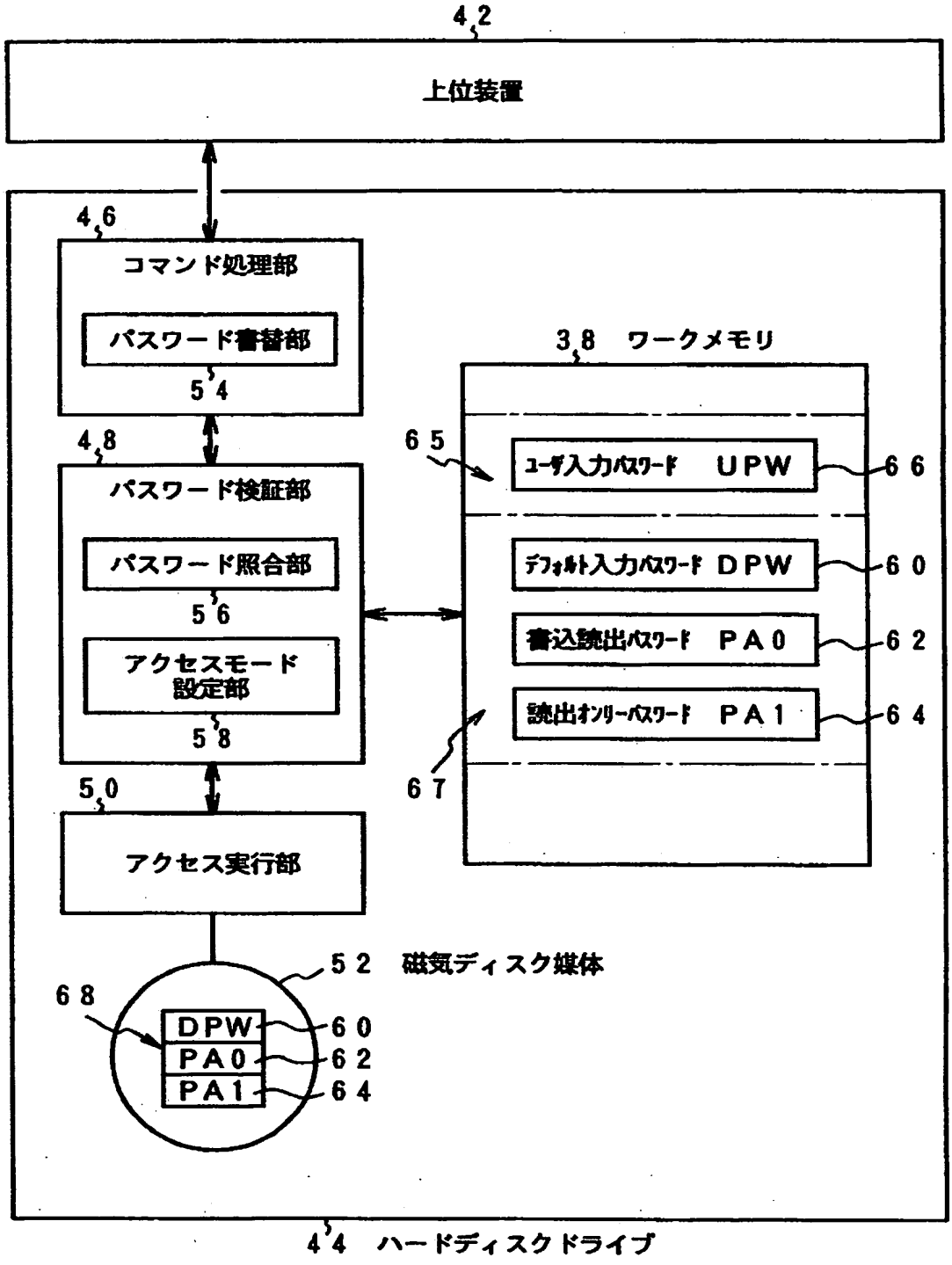
【図７】

本発明におけるパスワードの保存形式の説明図

保存形態	デフォルト入力パスワード格納位置	パスワード格納位置
1	ドライブ	ドライブ
2	媒体	媒体
3	ドライブ	媒体
4	媒体	ドライブ

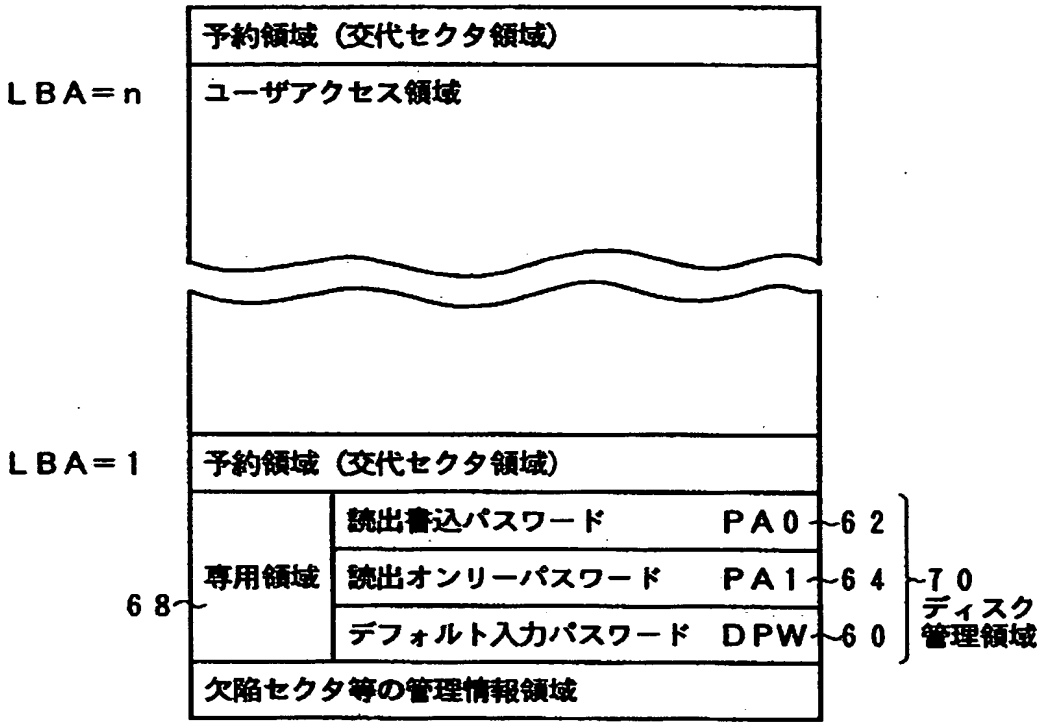
【図８】

パスワードを媒体のみに保存した本発明の実施形態の機能ブロック図



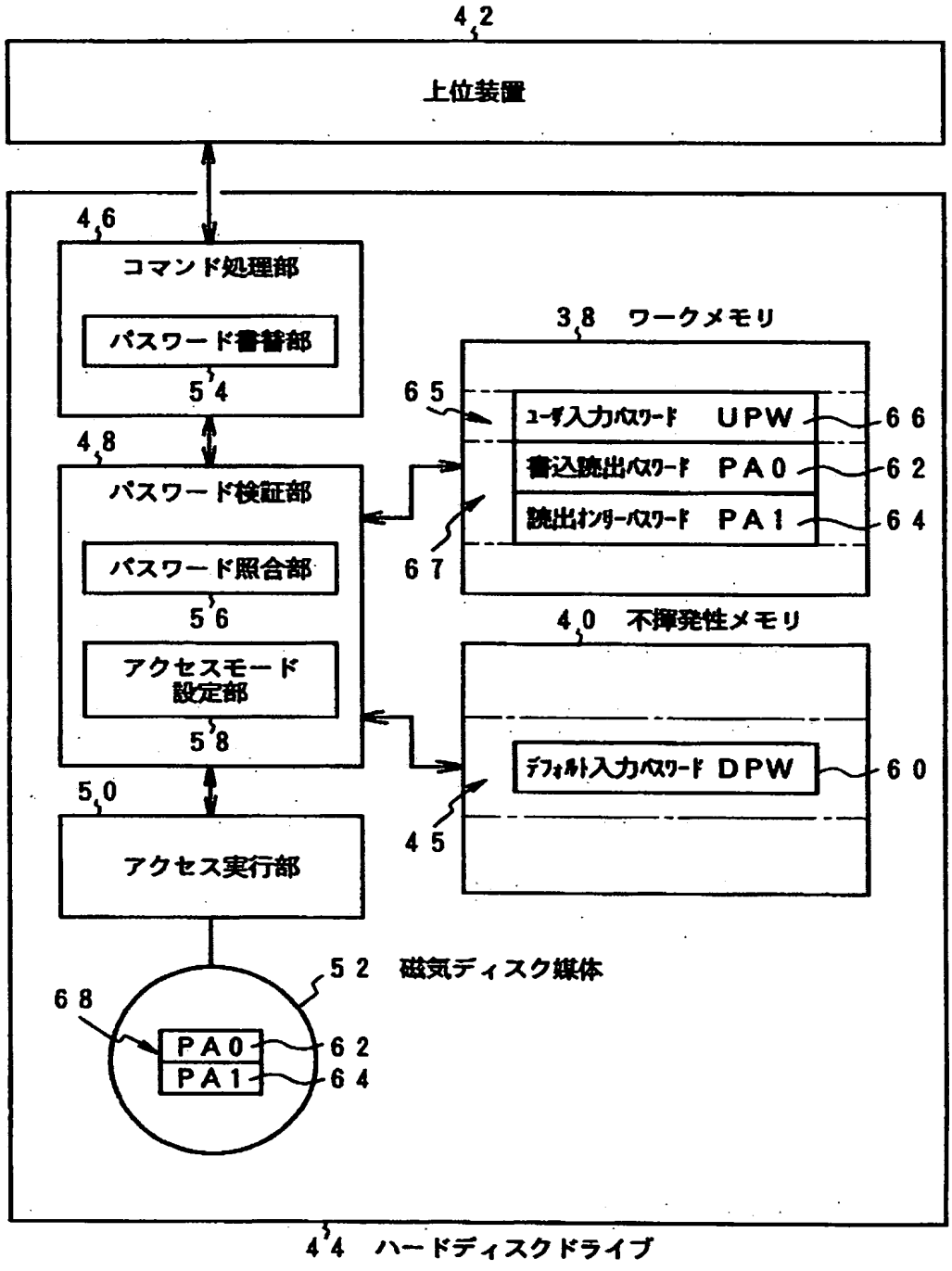
【図９】

図８の媒体内のパスワード保存領域の説明図



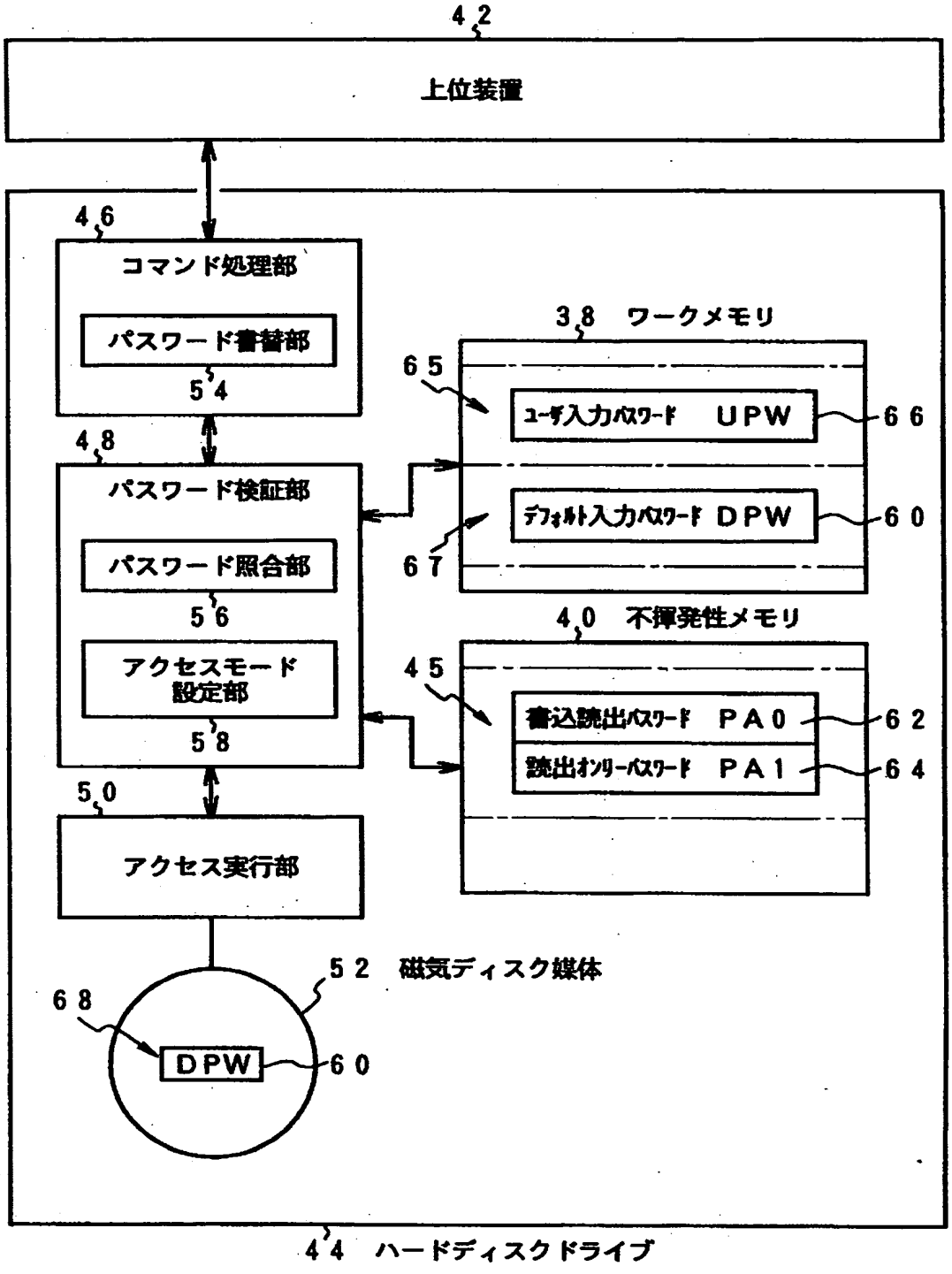
【図１０】

パスワードをドライブ本体と媒体に分けて保存した本発明の実施形態の機能ブロック図



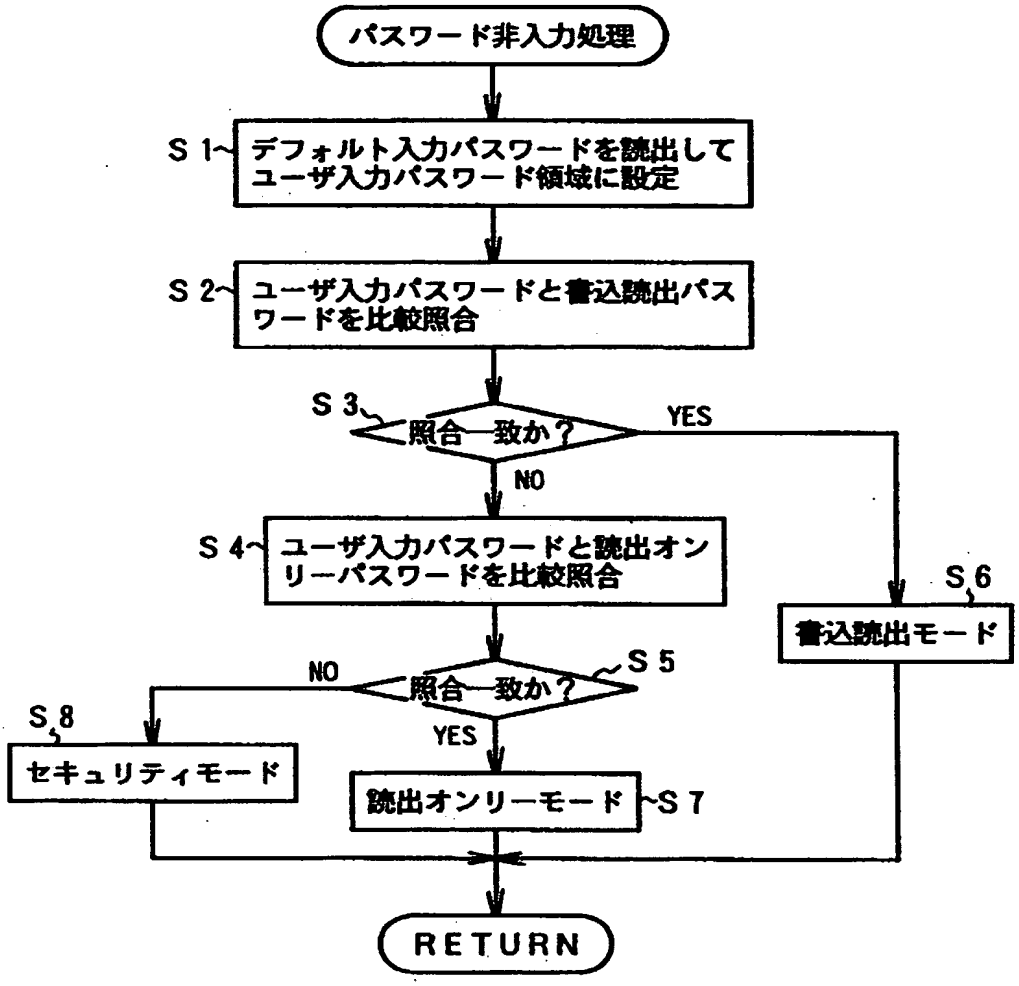
【図１１】

パスワードをドライブ本体と媒体に分けて保存した本発明の他の実施形態の機能ブロック図



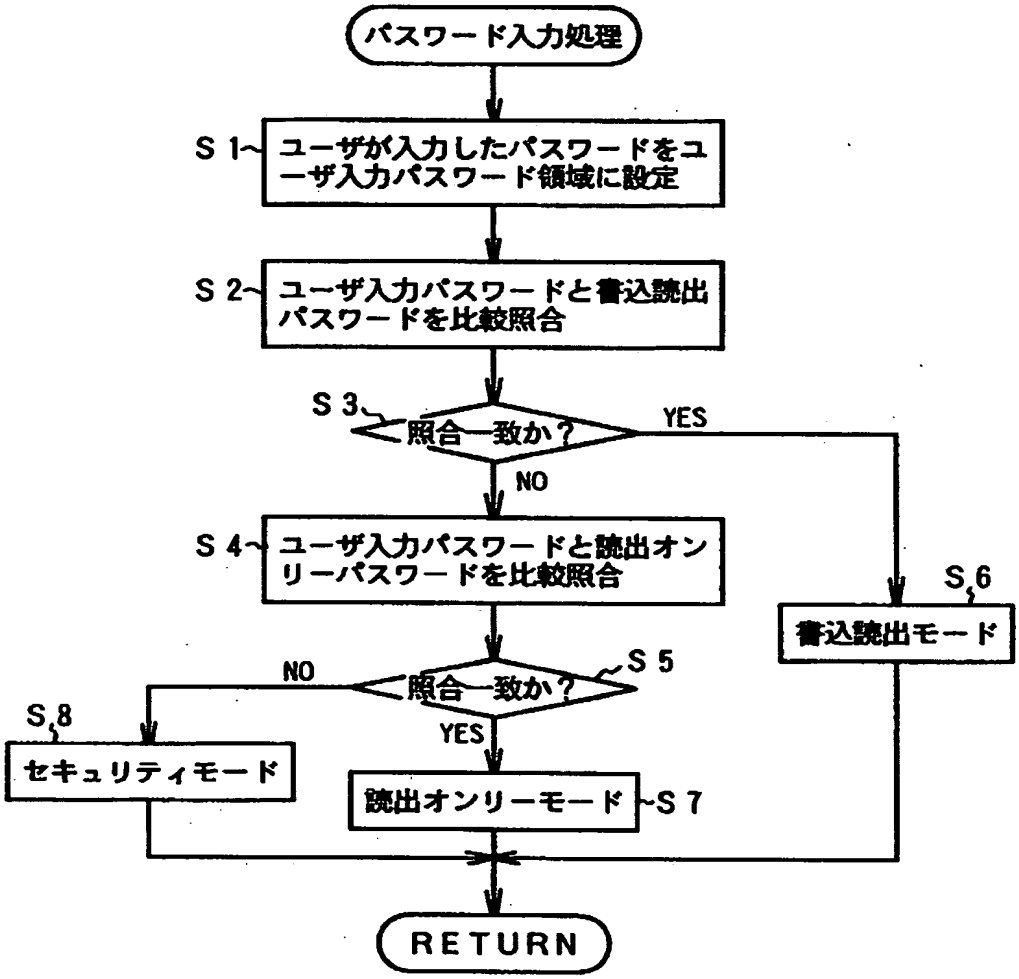
【図１２】

ユーザのパスワード入力がない場合のアクセス保護処理のフローチャート



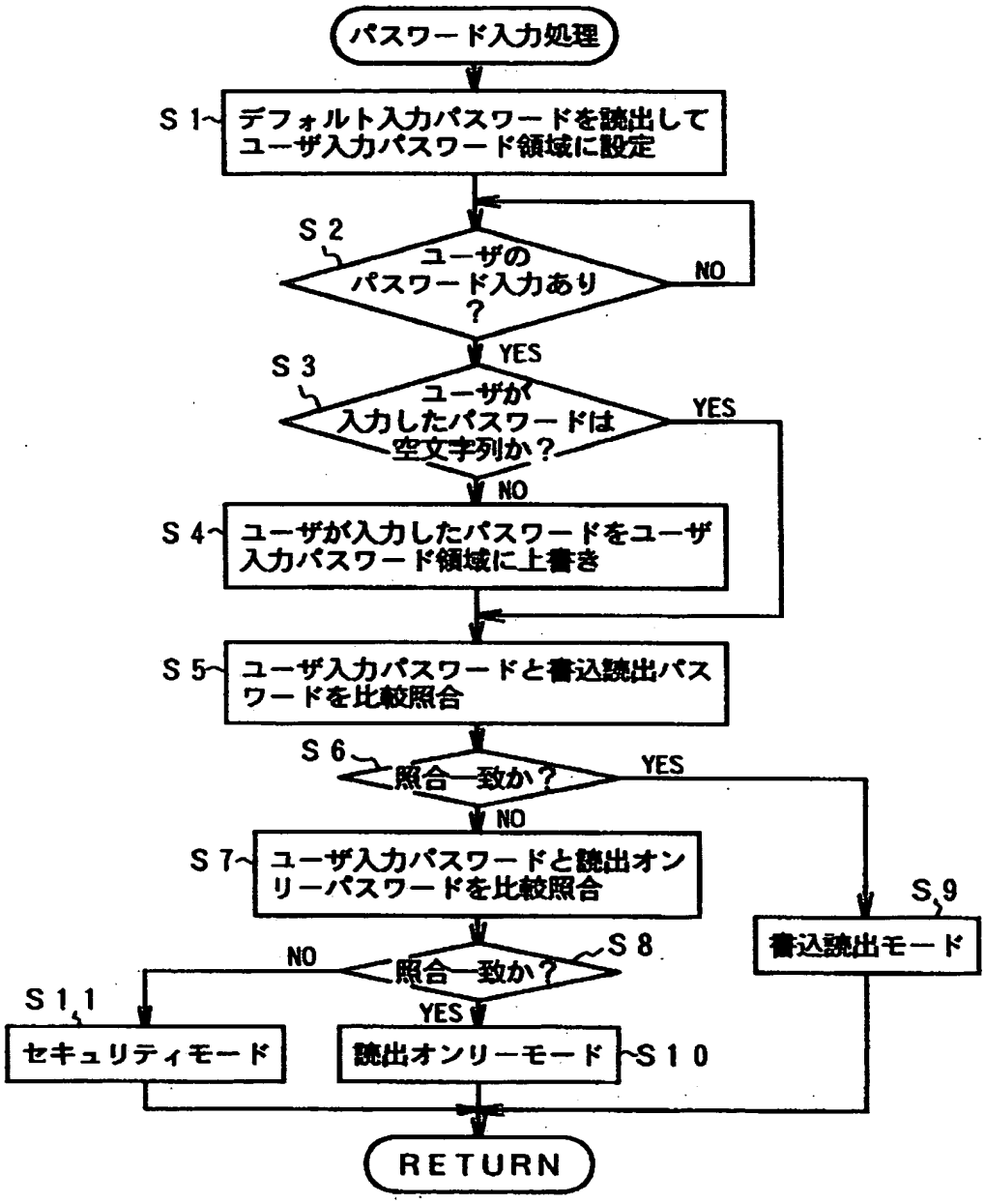
【図１３】

ユーザがパスワードを入力した場合のアクセス保護処理のフローチャート



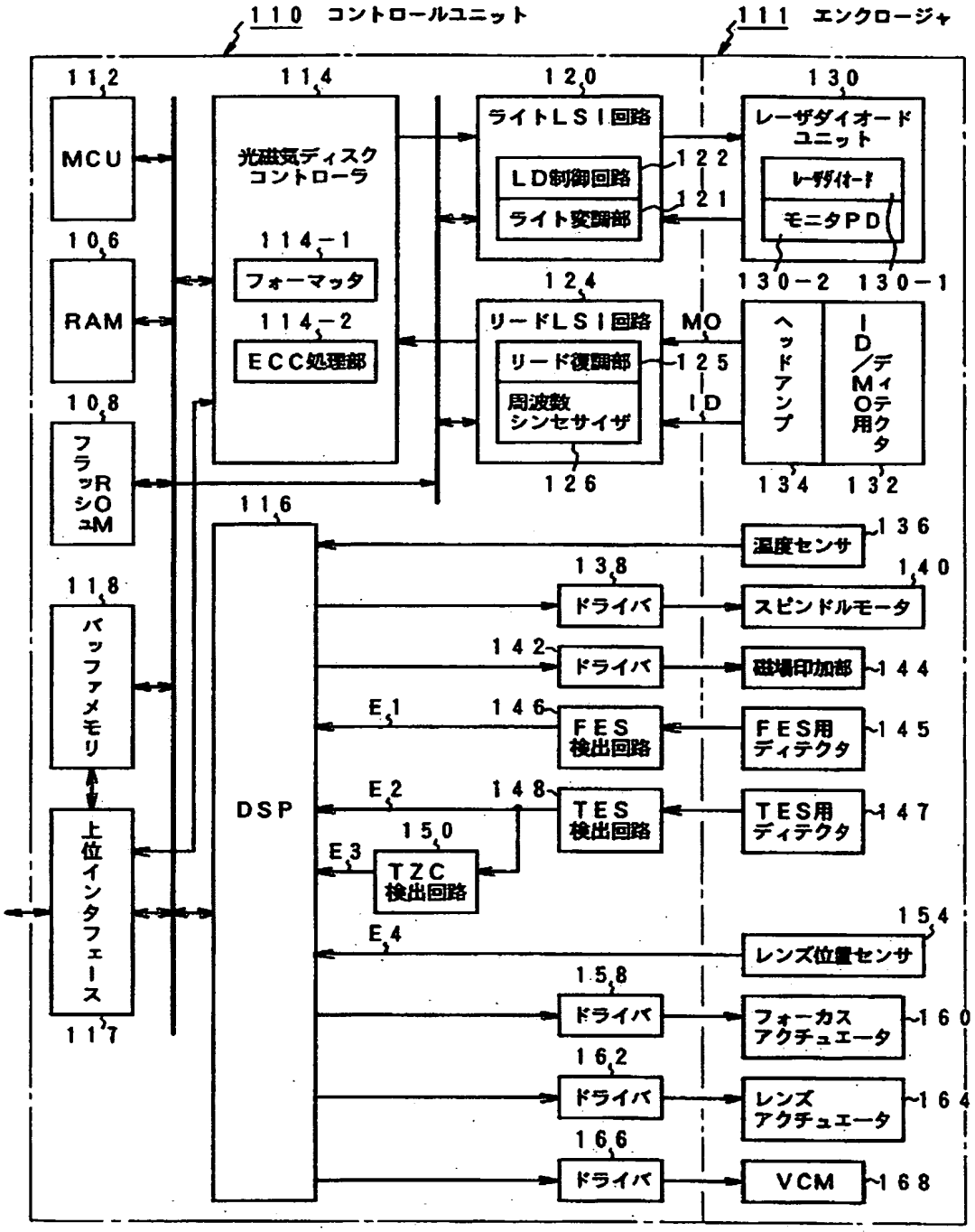
【図１４】

ユーザがパスワード入力操作を必ず必要とするアクセス保護処理のフローチャート



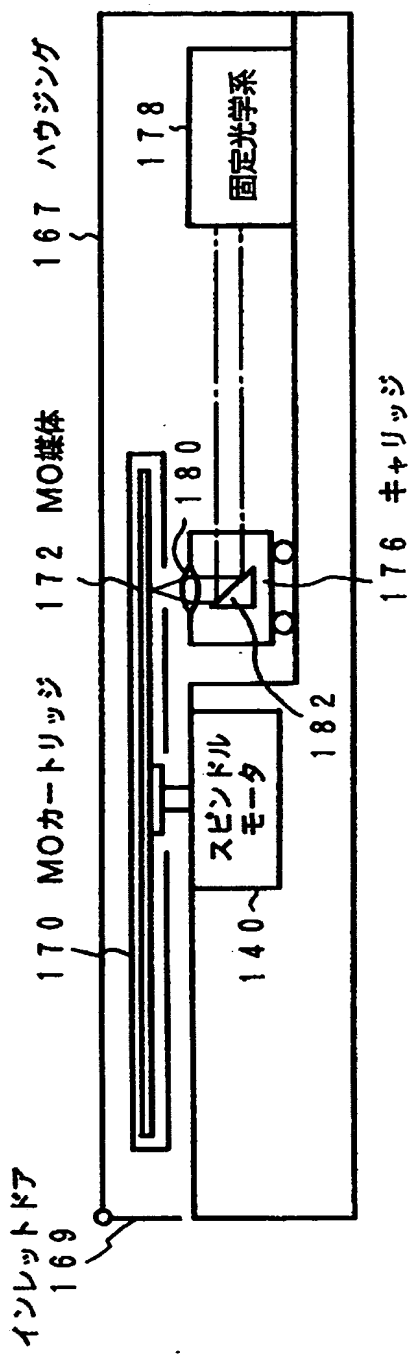
【図１５】

本発明が適用される光ディスクドライブのブロック図



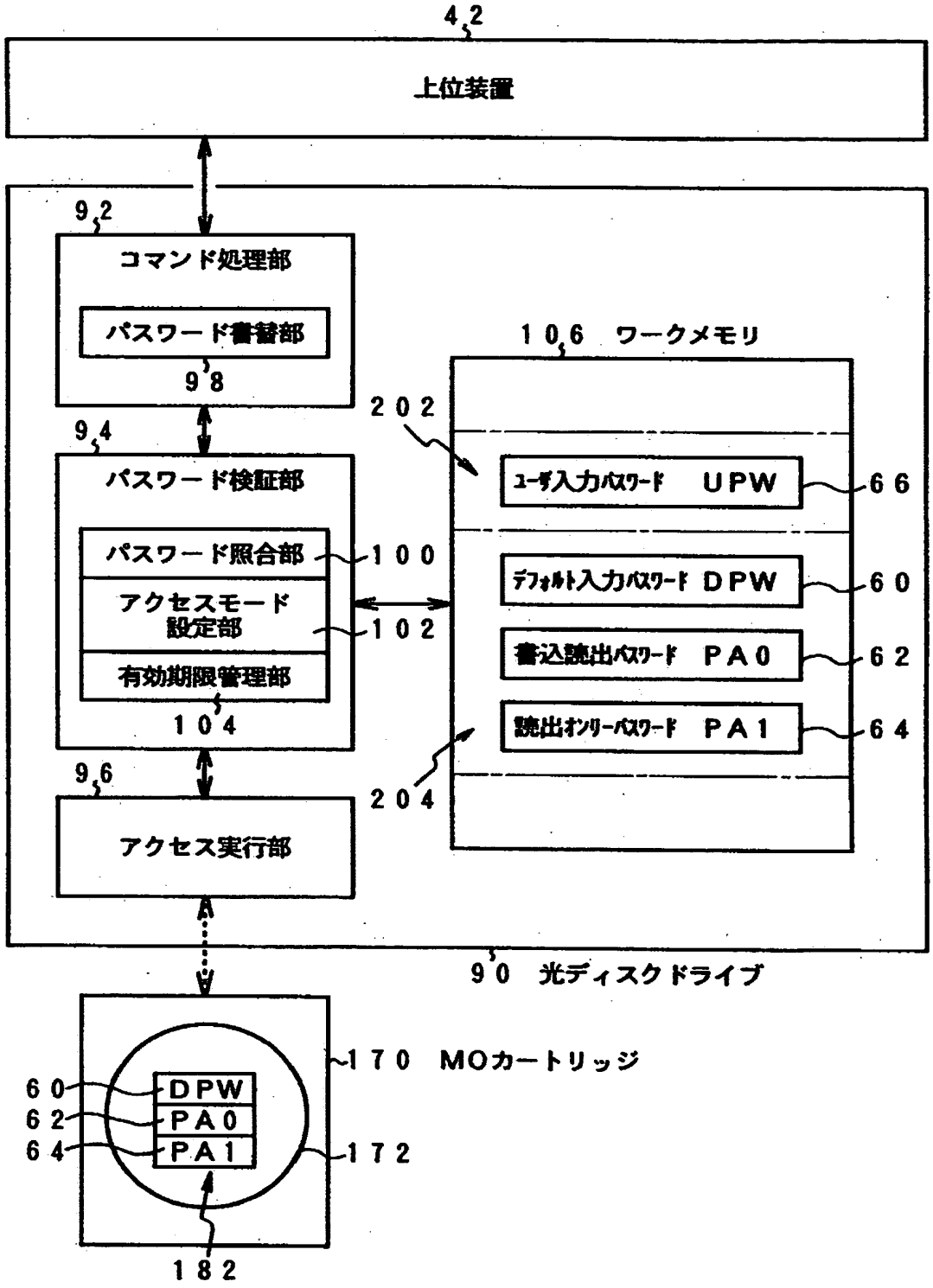
【図１６】

MOカートリッジをローディングした装置内部構造の説明図



【図１７】

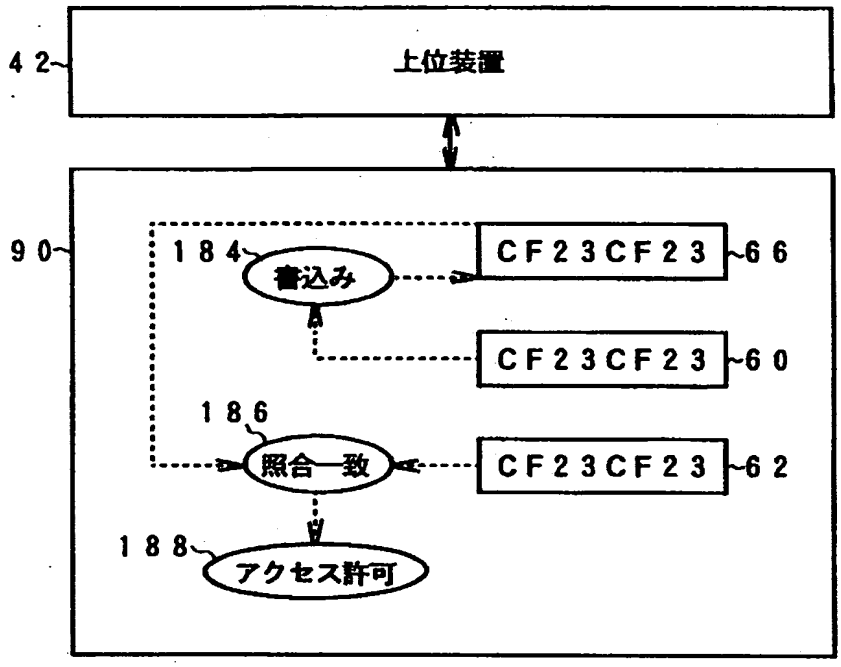
パスワードをリムーバブル媒体のみに保存した本発明の実施形態の機能ブロック図



出証特平１０－３０５６４４０

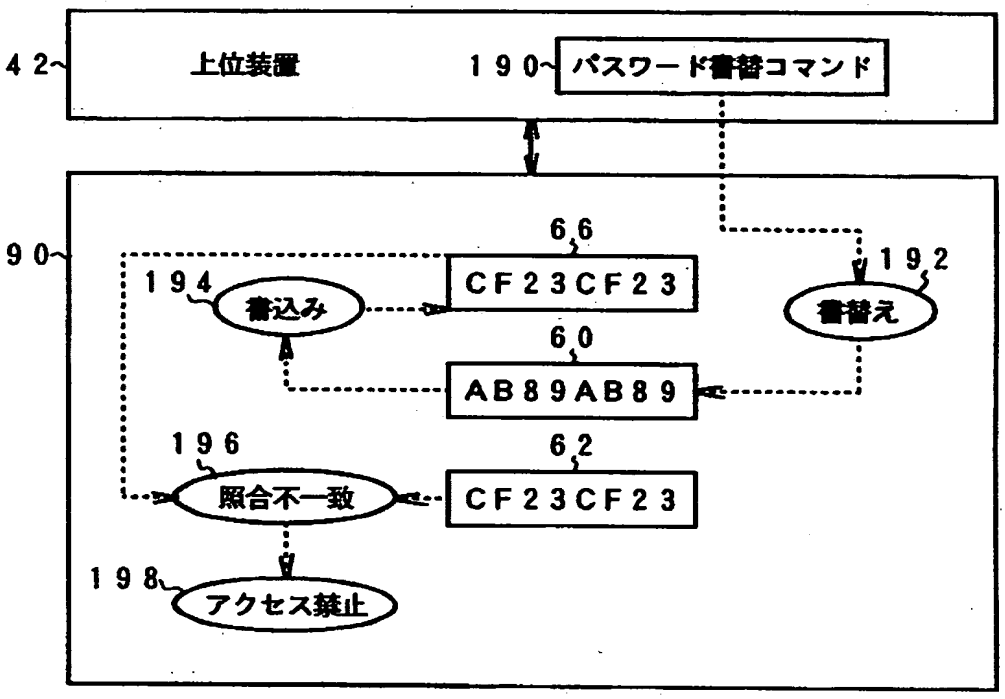
【図１８】

ＭＯドライブに対しユーザのパスワード入力がなくデフォルト入力パスワードでアクセス許可を獲得するアクセス保護処理の説明図



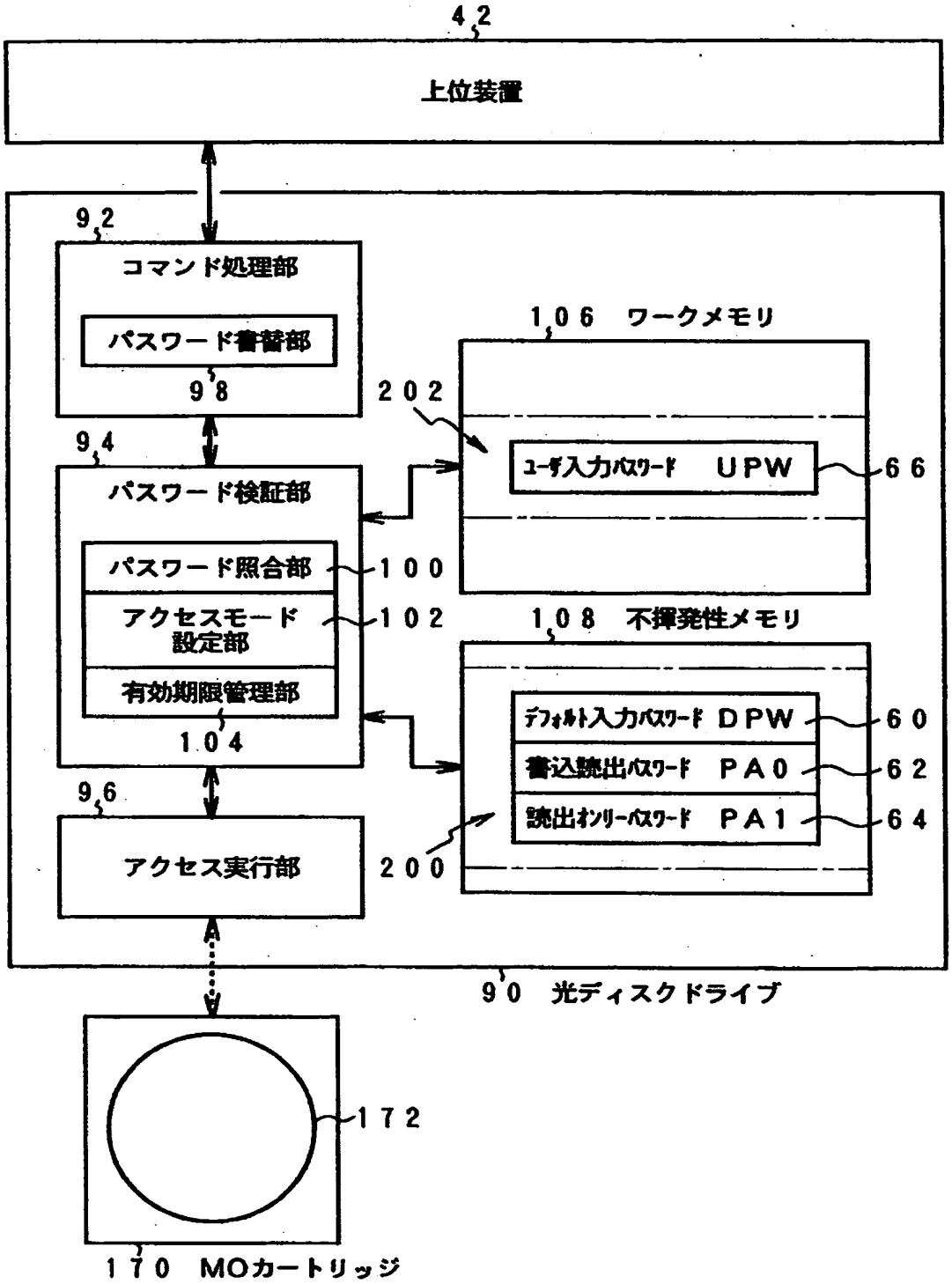
【図１９】

デフォルト入力パスワードによるアクセスを禁止するためのパスワード書替処理の説明図



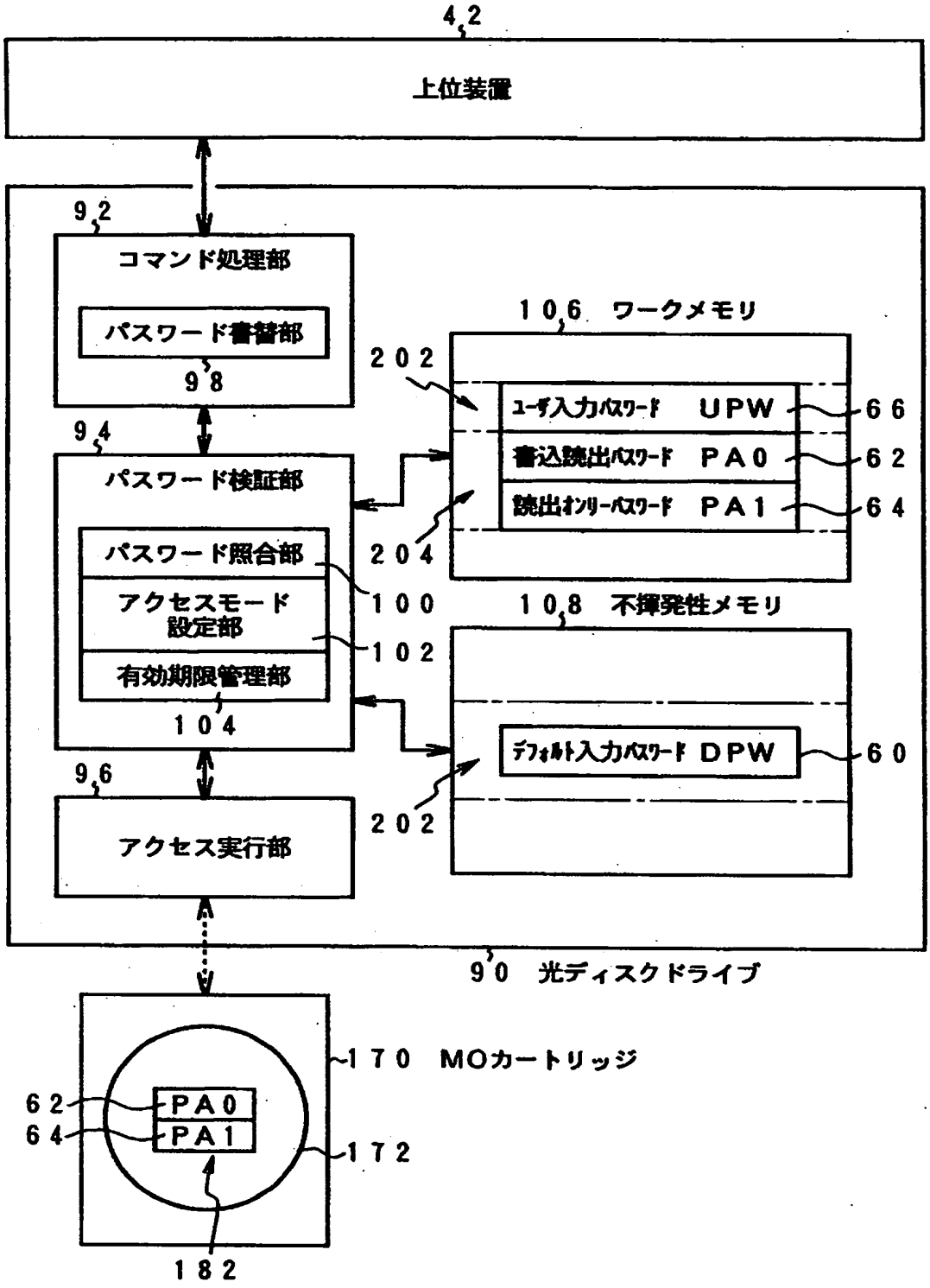
【図２０】

パスワードをMOドライブ本体に保存した本発明の実施形態の機能ブロック図



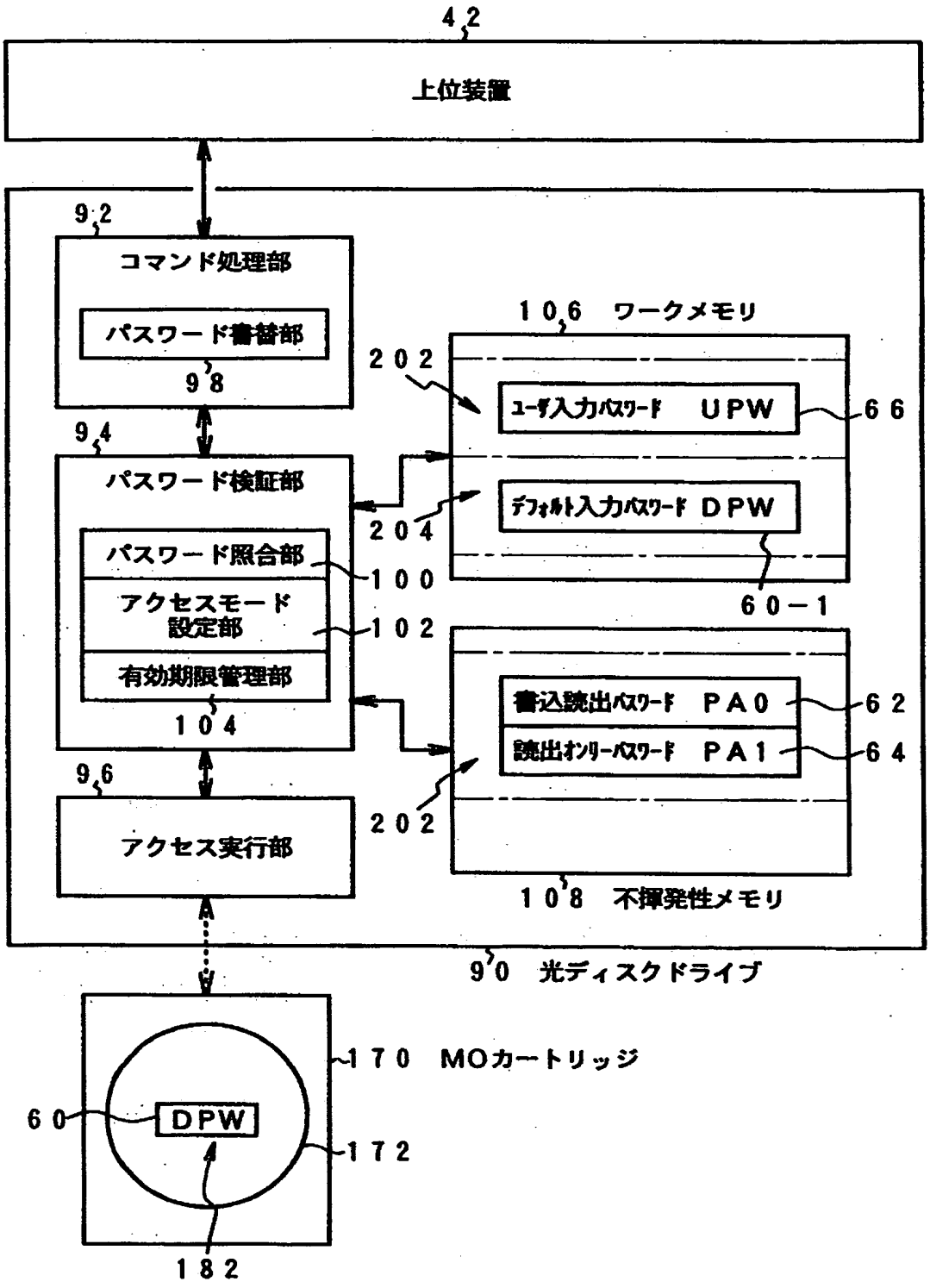
【図２１】

パスワードをMOドライブ本体とリムーバブル媒体に分けて保存した本発明の実施形態の機能ブロック図



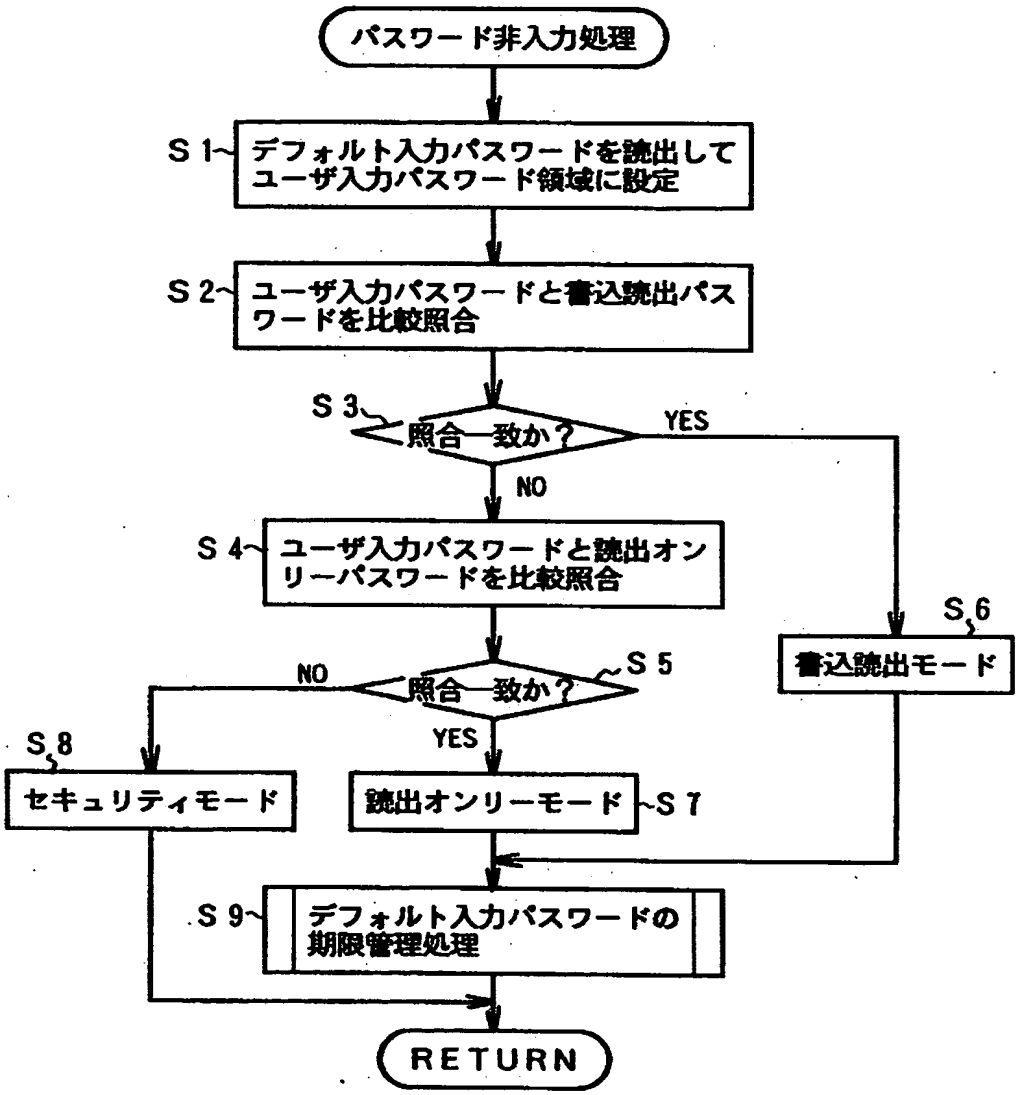
【図２２】

パスワードをMOドライブ本体とリムーバブル媒体に分けて保存した本発明の他の実施形態の機能ブロック図



【図２３】

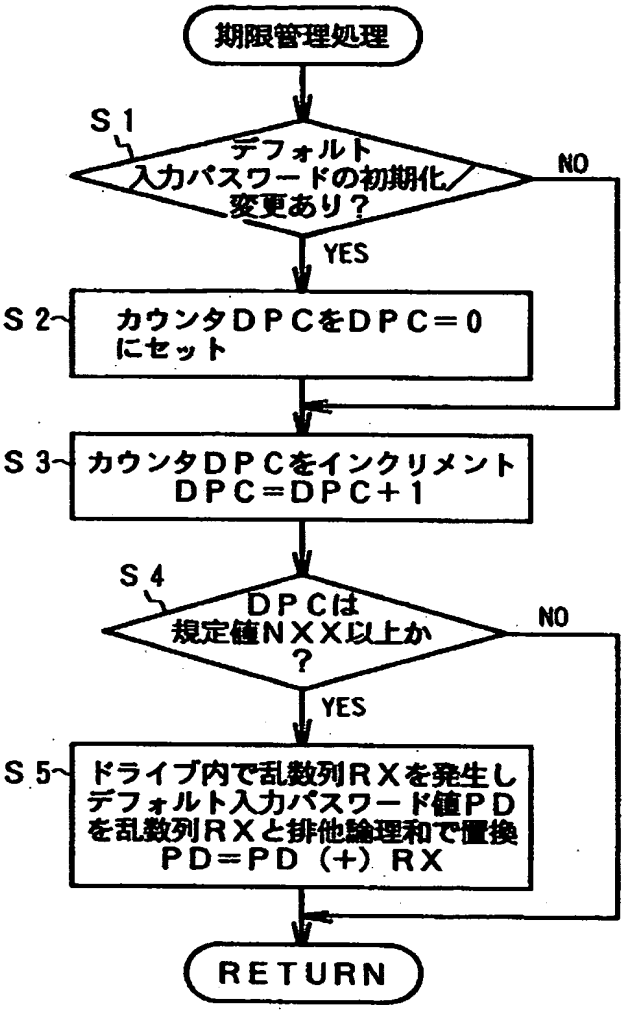
MOドライブにおけるユーザのパスワード入力がない場合のアクセス保護処理のフローチャート



【図２４】

カウンタで使用回数を計数してデフォルト入力パスワードの期限を管理する

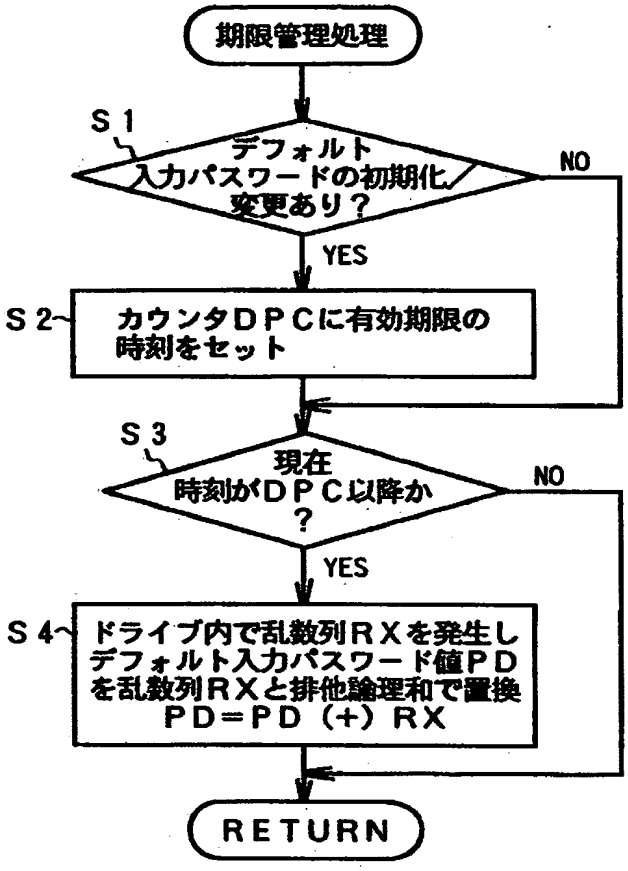
図２２の有効期限管理処理のフローチャート



【図２５】

デフォルト入力パスワードの期限となる時刻を設定して管理する

図２２の有効期限管理処理のフローチャート



【書類名】　　要約書

【要約】

【課題】パスワードによるアクセス保護を行っていても、ユーザのパスワード入力がなくともアクセスが許容され、パスワード入力の省略を可能とする。

【解決手段】デフォルト入力パスワード６０を保存し、ユーザからのパスワード入力がない場合はデフォルト入力パスワード６０をユーザ入力パスワード６６と見做してアクセス保護用パスワード６２との比較照合によりアクセス保護を制御する。このときデフォルト入力パスワード６０とアクセス保護用パスワード６２が同じ値であれば照合一致となり、ユーザのパスワード入力を必要とすることなくアクセスが許可される。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【代理人】　申請人
【識別番号】　100079359
【住所又は居所】　東京都港区西新橋３丁目２５番４７号　清水ビル８階
【氏名又は名称】　竹内　進
【選任した代理人】
【識別番号】　100093584
【住所又は居所】　東京都港区西新橋３丁目２５番４７号　清水ビル８階
【氏名又は名称】　宮内　佐一郎

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社

US 0915983307P1

Creation date: 10-30-2004
Indexing Officer: FNIGATU - FITSUM NIGATU
Team: OIPEBackFileIndexing
Dossier: 09159833

Legal Date: 06-05-2002

No.	Doccode	Number of pages
1	A...	1
2	SPEC	3
3	CLM	6
4	REM	12
5	XT/	1
6	IDS	1
7	LET.	1

Total number of pages: 25

Remarks:

Order of re-scan issued on .....